Washington State Department of Social and Health Services

Information Technology Security Policy Manual

Revision 5

December 1, 2003

Chapter 1: Introduction

1.1 PURPOSE

The purpose of the DSHS Information Technology (IT) Security Policy Manual is to provide information to establish a safe, secure environment for protecting the integrity and confidentiality of department data and for safeguarding department Information Technology resources.

1.2 SCOPE

A. IT security covers the protection of department data in any form, and the safeguarding of IT resources.

   1. The protection of data (both physical and electronic) includes:

      - Safeguarding the confidentiality of data recorded on any type of media (paper, magnetic, electronic, whiteboards, etc.),
      - Protecting the integrity of data, and
      - Ensuring the availability of data (proper backups, etc.).

   2. Protection of IT resources (equipment and software) include all measures needed to safeguard resources from theft, tampering, electrical hazards, and natural or manmade disasters.

   3. The physical protection of both data and IT resources includes measures restricting access, such as changing combinations to entry doors and safes.

B. The provisions of this manual apply to all DSHS employees, to contractors, and to other users who have access to department IT equipment or other IT resources. For binding service providers and contractors to the provisions of this manual, where appropriate, see Section 2.2.2 Contracting.

1.3 AUTHORITY

The Information System Services Division (ISSD) developed this manual by the authority of the DSHS Chief Information Officer (CIO) and DSHS Deputy Secretary.

1.4 SECURITY STRATEGY

The department's strategy for protecting the integrity and confidentiality of data and safeguarding IT resources contains five primary elements:

A. Maintaining a centralized capability to oversee the department wide IT security program;

B. Having appropriate security policies and procedures in place that are accessible by all department employees;

C. Requiring managers at all levels to enforce these policies and procedures;

D. Implementing a review process to ensure compliance with published policies and procedures; and

E. Implementing a reporting system that allows the DSHS Secretary to measure and report on organizational compliance with published security policy.

1.4.1 CENTRALIZED SECURITY ADMINISTRATION

A. Administrative Policy 15.10, Information and Resource Security, Paragraph A, requires the CIO to appoint an IT Security Administrator to administer the department's IT Security Program. This individual also serves as the ISSD IT Security Manager and manages the IT Security Section.

B. In accordance with Administrative Policy 15.10, Paragraph B, responsibilities of the IT Security Administrator include:

- Developing and maintaining the administrative policies related to the security of the department's information and IT resources;
- Maintaining the IT Security Policy Manual (this document) which documents the department's IT security policies and standards;
- Coordinating and administering federal and state IT security audits (see Chapter 9);
- Preparing and disseminating state and federal reports as required by statute (see Chapter 9);
- Developing and maintaining guidelines for Disaster Recovery Plans throughout the department (see DSHS IT Disaster Recovery Manual);
- Providing consultative and advisory services to managers and users throughout the department on matters pertaining to information and IT resource security, risk analysis and disaster recovery; and
- Providing ongoing information and IT resource security related training throughout the department (see Chapter 2).

1.4.2 IT SECURITY POLICIES AND PROCEDURES

The department's IT Security Program is based on various federal and state regulations. For a comprehensive listing of these regulations, including DSHS administrative policies relating to IT security, see DSHS IT Security References R1.4.2 IT Security Policies and Procedures.

1.4.3 RESPONSIBILITY FOR ENFORCING POLICY

Managers at all levels are responsible for enforcing compliance with IT security policies and required security measures (also see Section 2.2.9 Sanctions).

1.4.4 RESPONSIBILITIES OF ALL DSHS ORGANIZATIONS

The responsibilities of all DSHS organizations, as they relate to IT security, include the following:

A. Implementing the requirements described in this manual;

B. Conducting risk, threat, and vulnerability analyses, as described at Section 9.2.2 Risk, Threat, and Vulnerability Analyses;

C. Implementing and documenting security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, relating to the confidentiality, integrity, and availability of department data and systems.

1.4.5 EXCEPTIONS TO POLICY

Situations may occur or exist where meeting policy conflicts with business need. An exception to policy may be requested in writing. This request must detail the business need for the exception, the technical steps to be taken to address any security concerns, and the process and timeframe for implementing. All request should be addressed to the DSHS Chief Information Officer for approval.

1.4.6 REVIEW OF ORGANIZATIONAL SECURITY PRACTICES

DSHS is subject to a variety of federal and state IT security audits/reviews (see Chapter 9, Security Assessments, Reviews, and Reports).

1.4.7 MANDATORY REPORTS

The IT Security Section produces several mandatory security-related reports for DIS and the Internal Revenue Service (see Chapter 9).

1.5 EFFECTIVE DATE

This manual was originally issued in 1994
Revision 1 was effective June 30,1996
Revision 2 was effective March 1, 2001
Revision 3 is effective May 1, 2002

1.6 MANUAL FORMAT

A. This manual is organized into chapters, with each chapter covering a major topic of information and resource security. Most chapters are organized into two or three sections, as follows:

   1. The Introduction presents a chapter overview and, in some cases, a brief description of various topics discussed.

   2. The Policy section is divided into three parts, as follows:

      a. A policy statement – states what must be accomplished and, where applicable, the associated vulnerabilities and risks that make this policy necessary.

b. Standards – mandatory actions needed to mitigate risks and comply with policy statement.

c. Guidelines (optional) – recommended practices that, if adopted, will enhance security mandated by the policy statement.

B. Procedures and/or checklists are helpful for describing step-by-step processes required for some security related functions. A link to the applicable procedures will be provided at the appropriate place within this manual.

C. Online links are provided to appendices, where applicable, and to most reference documents.

1.7 REVISIONS

The Information System Services Division (ISSD) is responsible for revisions to this manual. It will be reviewed and revised annually, or more often as needed. ISSD will retain superceded versions of this manual for six years. Departmental organizational units may submit recommended changes to this manual to:

DSHS IT Security Administrator
Information System Services Division
MS: 45889

Interim updates that cannot be delayed until the next Manual update will be posted at the following ISSD web location:

http://techzone.dshs.wa.gov/ecenter/policies/policies.stm

1.8 DISTRIBUTION

This manual is only available online. Parts or this entire manual may be printed using available print functions.

Chapter 2: Personnel and Use of State Resources

2.1 INTRODUCTION

A. This chapter pertains to personnel-related policies and procedures for protecting information technology (IT) resources from misuse, and for protecting sensitive information from unauthorized disclosure or modification. It covers:

- Hiring,
- Security awareness and training,
- System Administrator training,
- Supervision and monitoring,
- Appropriate use of state resources, and telecommuting,
- Using privately-owned IT resources for state business, and
- Termination and transfer of employees.

B. Department personnel includes permanent or temporary employees, and other users who have access to department IT equipment or other IT resources.

2.2 POLICIES AND STANDARDS

2.2.1 HIRING AND APPROVING ACCESS

Policy Statement 2.2.1

Before deciding to hire personnel who may potentially have access to classified information or IT resources, or before approving their access, consider and, where appropriate, verify information obtained about the person during the hiring process e.g. information on the employment application, resume, or supplied during interviews.

Standards

S1. Verify information provided on employment applications to the extent possible. As a minimum, contact references during the hiring process.

S2. For employees who transfer, voluntarily or as part of the RIF process, contact their previous employer to determine if there maybe any issues with granting access to classified information.

2.2.2 CONTRACTING

Policy Statement 2.2.2

Before deciding to engage contractors who will use or have access to department IT equipment or other IT resources, and/or before approving their

access, obtain, consider, and/or examine, as appropriate, references or other information, and include required provisions in contracts.

Standards

S1. When contracting with personnel who will use or have access to department IT equipment or other IT resources:

a. Obtain, consider, and/or examine, as appropriate, references or other information about the contractor;

b. Provide in the contract that the contractor will be subject to the provisions of this manual, and to Administrative Policy 15.15 Use of Electronic Messaging Systems and the Internet.

c. In cases where the contractor will have access to confidential [classified] data, include in the contract the required elements of a data sharing agreement as described at section 3.2.4 Data Sharing Agreements.

2.2.3 IT SECURITY AWARENESS AND TRAINING

Policy Statement 2.2.3

All department employees and other users who have access to department IT equipment or other IT resources must receive annual security awareness training.

Standards

S1. All department employees must receive security awareness training when hired and annually thereafter.

S2. This training will include, at a minimum, the online, user-level, security awareness training provided by ISSD (HRDIS code 01-09-EG48). DSHS program areas may supplement this with program specific training.

S3. Security awareness training for employees will include:

a. Protecting the integrity and confidentiality of department data;

b. Password management, including procedures for creating, changing, and safeguarding passwords;

c. Guarding against, detecting, and reporting viruses and other malicious software;

d. Protecting department IT resources including the permitted use of equipment and software; and

e. Complying with commercial software licensing agreements (see Administrative Policy 15.12).

S4. Security awareness training will be reviewed annually, and updated as needed.

S5. The IT Security Manual and other pertinent directives regarding the use of IT resources must be made readily accessible to all department personnel.

S6. Contractors who have access to department IT equipment or other IT resources will be made aware of security requirements, via training, contract language, or other means as appropriate for the specific access they are granted.

2.2.4 IT STAFF TRAINING AND NON-DISCLOSURE AGREEMENTS

Policy Statement 2.2.4

IT staff with administrative rights to servers, workstations, applications, and/or data must be trained on security procedures. All IT staff, including those with administrative rights, will sign non-disclosure agreements.

Standards

S1. Before they assume their duties, IT staff with administrative rights to servers, workstations, applications, and/or data must be trained on security procedures relating to the scope of their responsibility.

S2. All IT staff, when hired and whenever their job duties change significantly, will sign non-disclosure agreements to only access or disclose information when appropriate and authorized.

Guidelines

G1. DSHS Form 03-374 (http://asd.dshs.wa.gov/forms/wordforms/word/03_374.doc) provides an example of a non-disclosure agreement for IT staff.

2.2.5 SEPARATION OF DUTIES AND SUPERVISION

Policy Statement 2.2.5

Take reasonable precautions to minimize the risk of financial fraud or theft, or of the mishandling of classified information, through separation of duties and supervision.

Standards

S1. Design program area workflow to provide as much separation of sensitive functions as possible.

S2. Actively supervise and review employee efforts where confidential data or the potential for committing fraud exists.

S3. Rotate employees in sensitive positions where practical, unless administrative or system checks and balances are in place. Periodic job rotation minimizes the potential for an employee to commit fraud.

S4. Ensure that the annual Risk Assessment/Self-Evaluation (RASE), Section XII. Information Systems, is reviewed by someone not directly responsible for implementing the system under review.

Guidelines

G1. DSHS organizations should consider the possible need for supervising personnel, such as janitorial staff, who may require physical access to a facility, but who are not authorized to access confidential data.

2.2.6 APPROPRIATE USE OF STATE RESOURCES AND TELECOMMUTING

Policy Statement 2.2.6

Take reasonable precautions to ensure that state resources are used only for those purposes allowed by state and department policy. See DSHS IT Security References R2.2.5 Usage Template, for an example of Appropriate Use Statement.

NOTE: This policy applies to contractors and other users who have access to department IT equipment or other IT resources. Appropriate use statements must be spelled out in contracts, as required by section 2.2.2 Contracting.

Standards

S1. See WAC 292-110-010, Use of State Resources, and Administrative Policy 15.15, Use of Electronic Messaging Systems and the Internet, Section B, for restrictions on the use of state resources including:

a. The general requirement to use state resources for state business, and

b. The limited conditions under which state resources may be used for personal purposes

S2. Department personnel must not:

a. Attempt to gain unauthorized access to any information system, or attempt to capture or otherwise attempt to obtain passwords, encryption keys, or any other access control mechanisms that could allow them unauthorized access; or

b. In any way cause unauthorized alteration to, damage to, or disruption of the operations of any information system, e.g. deliberately spreading viruses, or making another network unusable by launching a denial of service attack.

S3. Supervisors may authorize home use of departmental equipment for official business in accordance with the provisions of Personnel Policy 590, V.F Teleworking/Flexible Work Hours, Computer equipment/information.

Guidelines

G1. Home use of computers requires adequate maintenance of patches, anti-virus software, etc. This is true for both departmental equipment and employee owned computers. This should be coordinated with the appropriate IT staff.

2.2.7 USING PRIVATELY-OWNED IT RESOURCES FOR STATE BUSINESS

Policy Statement 2.2.7

Unless prohibited by division policy, the use of privately owned IT resources to conduct state business may be authorized.

Standards

S1. Unless otherwise prohibited by Division policy, supervisors may authorize the use of privately owned software and personal computers, printers and similar hardware at work, provided:

a. Before being used, the software is checked for viruses by local or divisional IT staff.

b. The employee acknowledges in writing that liability for loss or damage to privately owned IT equipment and software is not assumed by the state.

2.2.8 TERMINATION AND TRANSFER OF EMPLOYEES

Policy Statement 2.2.8

When an employee or other system user terminates employment, transfers, or changes duties, access that is no longer needed or appropriate must be promptly revoked. The employee must be reminded of his or her duty to keep information confidential.

Standards

S1. When an employee is terminated for cause, revoke all access immediately. This may include not having the employee come into the office at all.

S2. When an employee is transferred, deactivate his or her account for a maximum of six months (30 days preferred), after which the account must be terminated if the employee does not return.

S3. When an employee has a change of duties, remove privileges that are no longer needed.

S4. Remind the employee in writing of his or her continuing responsibility to maintain the confidential nature of programs, data and processes to which they have had access. Place a copy of the document in the individual's personnel file.

2.2.9 SANCTIONS

Policy Statement 2.2.9

Managers will enforce department IT Security policies by applying appropriate sanctions against employees and others who have access to department information systems, who fail to comply with those policies. Criminal sanctions that result from illegal activities are applied by the appropriate court system. Managers' responsibilities may be limited to reporting incidents that merit a legal investigation.

Standards

S1. When an employee fails to comply with department IT security policies or standards, then their manager will apply appropriate sanctions for the type and frequency of the offense.

Guidelines

G1. Sanctions may range from a verbal warning, up to, and including dismissal. As noted above, legal sanctions are the responsibility of the court system. These penalties are defined in State law, or in Federal legislation (HIPAA, Federal Tax Code, Social Security Act, etc.)

Chapter 3: Classifying and Protecting Data and IT Resources

3.1 INTRODUCTION

A. This chapter covers:

- Classifying and protecting the confidentiality and integrity of department data,
- Physical and environmental controls over IT equipment,
- Storage media,
- Work areas, and
- Compliance with licenses for copyrighted material.

Privacy is protecting the confidentiality of personal information about employees and department clients. Privacy issues should be referred to the DSHS Privacy Officer for disposition in accordance with Administrative Policy 15.16, Privacy Policy – Safeguarding Personally Identifiable Information.

3.2 POLICIES AND STANDARDS

3.2.1 CLASSIFY DATA ACCORDING TO LEVEL OF PROTECTION NEEDED

Policy Statement 3.2.1

Managers must ensure that data entrusted to their care is classified according to the four broad categories described below, and protected accordingly:

Category 1 – Public information

Public information is information that can be released to the public. It does not need protection from unauthorized disclosure, but does need protection from unauthorized change that may mislead the public or embarrass DSHS.

Category 2 – Sensitive Information

Sensitive information is not specifically protected by law, but should be limited to official use only.

Category 3 – Confidential Information

Confidential information is information that is specifically protected by law. It generally includes:

a. Personal information about individual clients, regardless of how that information is obtained.

b. Information concerning employee payroll and personnel records.

c. Source code of certain applications programs that could jeopardize the integrity of department data or result in fraud or unauthorized disclosure of information if unauthorized modification occurred.

Category 4 – Information Requiring Special Handling

Information requiring special handling is information for which:

a. Regulations or agreements dictate especially strict handling requirements; or

b. Serious consequences could arise from unauthorized disclosure ranging from life threatening to legal sanctions.

For examples of Special Handling information, see DSHS IT Security References R3.2.1 Classify Data According to Level of Protection Needed.

NOTE: To reduce repetition in this manual, the terms “classified data” and “classified information” are used to collectively denote categories 2 through 4.

Standards

S1. All applications must be designed to protect the highest category of data that will be processed by the application.

3.2.2 GENERAL PROTECTION REQUIREMENTS

Policy Statement 3.2.2

Managers must ensure that data entrusted to their care is protected according to the appropriate category described above.

Standards

S1. Public disclosure of information must be in accordance with the Public Records Disclosure Act, RCW 42.17.250 through 42.17.340.

S2. Protect the integrity of data, including public information, to preclude unauthorized changes.

S3. Reproduce documents containing **classified** information only to the extent necessary to accomplish the department's mission.

S4. Restrict the use of classified information to employees who have a need to know in the performance of their assigned duties.

3.2.3 PROTECTING CLASSIFIED DATA IN DOCUMENTS AND ELECTRONIC MEDIA

Policy Statement 3.2.3

Adequate controls and safeguards must be in place to prevent unauthorized access to classified documents and to prevent the loss or unauthorized

access to classified information stored on removable media and computer hard drives (contained in servers, workstations, network storage devices, etc). Removable media includes magnetic tapes, cartridges, ZIP disks, CDs, etc.

Standards

S1. Store documents and removable media that contain data requiring **special handling** in locked containers when not in use.

S2. Do not leave documents or removable media containing **confidential** or **sensitive** information unprotected after normal working hours.

S3. Do not leave documents and removable media containing classified information unattended in areas readily accessible to the general public.

S4. For electronic media containing protected health information (PHI), maintain inventory records showing physical movement, and persons responsible (i.e. the movement of hard drives containing PHI in and out of machines, and the physical movement of tapes, CDs, Zip-disks, etc. containing PHI).

S5. For machines containing classified data, including servers, network storage devices, and other electronic devices, maintain inventory records showing physical movement, and person(s) responsible.

S6. Do not commingle classified documents with routine documents (documents should be separated into different folders or directories.)

Guidelines

G1. Administrations may choose to track more than just protected health information, for simplification.

3.2.4 DATA SHARING AGREEMENTS

Policy Statement 3.2.4

Data sharing agreements must be a formal contract, and be reviewed by the DSHS IT Security Administrator.

Standards

S1. The sharing of classified data with an entity external to DSHS must be covered by a formal contractual agreement.

- Data will not be shared until a signed, formal contractual agreement is in place.
- The agreement must be processed through the Agency Contracts Database (ACD) managed by the DSHS Contracts section.
- The DSHS IT Security Administrator must review these agreements.

- Sharing of data may be the primary focus of a contractual agreement, or it may be only part of the agreement, e.g., the contract is for services rendered, and the specified services require access to department data.

S2. The agreement must:

- Specify what data is to be shared, how it will be accessed, what the data will be used for, and what will be done with the data once the external entity is finished with the data;
- Require appropriate protection of data;
- Include required language as specified at DSHS IT Security Procedures P3.2.4.S2 Data Sharing Agreements—Required Language.

NOTE: If contractor staff will have access to department IT equipment or other IT resources, then the contract must make those staff subject to the provisions of this manual, and to Administrative Policy 15.15 Use of Electronic Messaging Systems and the Internet, as required by section 2.2.2 Contracting.

S3. Upon becoming aware of a material breach of the agreement, department staff will take appropriate enforcement or reporting action. See DSHS IT Security Procedures P3.2.4.S3 Data Sharing Agreements—Violations.

S4. Data sharing agreements are required only when sharing department data with an entity external to DSHS. Sharing of data within DSHS can be accomplished using an informal agreement (such as a memorandum of understanding (MOU)).

3.2.5 DESTRUCTION OF CLASSIFIED INFORMATION

Policy Statement 3.2.5

When no longer needed, classified information must be disposed of in a manner that prevents unauthorized disclosure of the information.

Standards

S1. Destroy documents containing classified information in a manner that prevents unauthorized disclosure of their contents.

a. For documents containing sensitive or confidential information, a contract with a recycling firm to recycle confidential documents is acceptable providing the contract assures the confidentiality of data will be protected.

b. For documents containing information that is classified as special handling required, recycle is not an option. These documents must be destroyed by shredding, pulping, or incineration.

S2. Destroy CDs that contain classified information by incineration or completely defacing the readable surface with a course abrasive. Special shredders are available for destruction of CDs, which is an acceptable alternative.

S3. Destroy data on magnetic tapes by degaussing.

S4. Destroy data on ZIP disks and similar devices by zero filling, wiping, or physically destroying disks by cutting them up.

S5. Destroy floppy disks by cutting them up.

3.2.6 SPECIAL PROCEDURES FOR COMPUTER HARD DRIVES

Policy Statement 3.2.6

When computers are transferred, surplused, or sent in for repair, any classified information residing on the computer's hard drive must be disposed of in a manner that prevents unauthorized disclosure of the information.

Standards

S1. To remove ("wipe") classified information from a hard disk, use a utilities program, such as Norton Utilities, or similar method. One pass should thwart reasonable efforts to gain access to the data. Simply deleting the files does not remove the data.

S2. Before the computer is released for surplus or transferred to another employee who does not have a need to know, remove classified information by:

a. "Wiping" it from a hard disk as described above; or
b. Removing the hard drive if it contains data requiring special handling.

If the computer is defective and being surplused, remove and destroy the hard drive if it contains confidential data, or "wipe" the hard drive before putting into another computer.

S3. If the repair of a machine precludes the removal of sensitive or confidential information, require the repair vendor to sign a statement of confidentiality, or require the repair to be done in the presence of a security-aware employee.

S4. Hard drives containing special handling information must be removed and stored in a secure area before the PC is released for repair.

3.2.7 PROTECTING IT EQUIPMENT

Policy Statement 3.2.7

Adequate physical and environmental controls must be in place to prevent loss or damage to IT equipment and other IT resources.

Standards

S1. Ensure adequate safeguards and controls are in place to prevent equipment and other IT resources from being physically removed from the premises without authorization.

S2. Protect modems, patch panels, hubs, switches, network gateways, and file server equipment from tampering and accidental damage. As much as possible, centralize equipment in locked rooms.

S3. Plug all equipment into a UL certified surge control device.

S4. Never plug coffee pots, hot plates, vacuums, laser printers, or other non-computing devices into a surge control device serving computing equipment.

S5. Locate a portable fire extinguisher, suitable for extinguishing electrical fires, near data processing equipment.

3.2.8 WORKSTATION COMPUTERS

Policy Statement 3.2.8

Take reasonable precautions to protect data stored on workstation computers.

Standards

S1. Whenever possible, store classified information on LAN servers rather than on workstation computers. In cases where classified information must be stored on a workstation, a higher level of security must be implemented, including:

- Maintaining inventory records, as described at Section 3.2.3 Protecting Classified Data In Documents and Electronic Media;
- Following special procedures when computers are transferred, surplused, or sent in for repair, as described at Section 3.2.6 Special Procedures for Computer Hard Drives.

S2. Control access to department workstation computers with passwords or stronger authentication devices.

S3. When a workstation computer is operational, access to the computer, and the data contained on that computer, must be protected as follows:

a. Manually lock the workstation before leaving your work area (contact your computer support staff for details); and

b. Use a screen saver, with password, that is set to activate after no more than 20 minutes of inactivity.

Guidelines

G1. An appropriate usage template (see DSHS IT Security References R2.2.5 Usage Template) should be displayed on the screen when logging into a workstation, or accessing a DSHS intranet homepage.

3.2.9 PORTABLE COMPUTING DEVICES

Because of their small size and high value, portable computing devices (e.g. laptops, handhelds, personal digital assistants (PDA), etc.) are particularly subject to theft, which can result in not only the loss of a valuable piece of equipment, but the compromise of confidential information or secret codes, as well.

Policy Statement 3.2.9

Portable computing devices must be given special protection.

Standards

S1. Encrypt any classified information or dial-in connection information stored in a laptop computer (see Chapter 8, Encryption and Data Integrity.)

S2. Use hardware-based passwords to protect access to portable computing devices when available. Do not store classified information on a portable device where the data cannot be encrypted, or protected by a hardware-based password. (Encryption is the preferred method of protection, when available.)

S3. Physically protect portable computing devices by:

a. Keeping them in locked storage when not in use,

b. Using check-in/check-out procedures when they are shared; and

c. Taking frequent inventories.

S4. When traveling, keep portable computing devices under your control.

NOTE: For backup requirements, as they relate to portable computing devices, see Section 3.2.12 Backup and Recovery of Department Data.

3.2.10 WORK AREAS

Policy Statement 3.2.10

Adequate controls must be in place to restrict unauthorized access to work areas.

Standards

The following standards apply to work areas that contain classified information, or information and systems whose integrity and availability are mission-essential

S1. Lock entrances to work areas when vacant.

S2. Limit access to work areas to authorized employees and visitors. Visitors must be escorted. Position computer monitors to prevent inappropriate viewing by non-DSHS personnel, for example clients at a counter, or persons outside a window.

S3. Change lock combinations/access codes at regular intervals.

S4. Document repairs and modifications to the physical components of a facility that are related to security (for example: security systems, walls, doors, and locks). For leased facilities, lease agreements should require the ability to access maintenance records. These records must be kept for five years back from the current date.

S5. Upon termination of employees, recover keys and key cards; and change door lock and safe combinations as soon as possible, but in no case later than 30 days from the effective date of the change.

Guidelines

G1. Replace keypads and key locks with key card systems to facilitate access control.

3.2.11 COPYRIGHTED MATERIAL

Policy Statement 3.2.11

Adequate controls must be in place to ensure the prevention of unlawful acquisition, reproduction, distribution or transmission of computer software (see Administrative Policy 15.12, Protecting Computer Software, for detailed policy governing the use of software in DSHS).

Standards

S1. Employees will comply with the provisions of licensing agreements and/or copyrights governing the use of computer software.

3.2.12 BACKUP AND RECOVERY OF DEPARTMENT DATA

Policy Statement 3.2.12

Establish policies, plans, procedures, and test strategies for the backup and recovery of systems and data.

Standards

S1. Organizational entities that have an IT function must have an IT Disaster Recovery Plan. Plans must be constructed according to the instructions contained in the DSHS IT Disaster Recovery Manual, tested annually, and updated as needed.

S2. Disaster recovery plans must include provisions for protecting classified information.

S3. Back up all mission-essential and production data, including messages on e-mail servers, on a regularly scheduled basis (at least once each week), and before equipment is moved. Retain copies of backup media using the Grandfather, Father, Son rule to ensure a complete recovery following an incident. This does not preclude retaining more than three iterations.

For an explanation of the Grandfather, Father, Son rule, see DSHS IT Security References R3.2.12 Grandfather, Father, Son Rule.

S4. Store backup copies of data and software at a secure off-site facility.

S5. Mission-essential data will normally be stored on a server rather than on a workstation, to facilitate backup and recovery. In exceptional cases where this data must be stored on a workstation or device other than a server, make special provisions to ensure backups as detailed above.

Chapter 4: Access Security, Identification, & Authentication

4.1 INTRODUCTION

This chapter covers policies for restricting access to data and/or applications/ programs residing on all computers, including mainframes, local area networks, client servers, or stand-alone personal computers.

NOTE: For the purpose of this manual, user ID and log-on ID are synonymous. The user ID identifies the operator to the computer, and the password verifies that the person is who they claim to be. The user ID is not considered confidential, while a password is considered secret.

4.2 POLICIES, STANDARDS, AND GUIDELINES

4.2.1 GENERAL ACCESS REQUIREMENTS

Policy Statement 4.2.1

Adequate controls must be in place to prevent unauthorized access to department computers and data.

Standards

S1. Divisions must formally appoint one or more IT security administrators for protecting access to their data and computer systems (See Chapter 12, Mainframe Security and MAPPER, for mainframe security administrators).

S2. Caretakers of department data must approve access to data under their control. Access may be granted on an individual or group/role basis.

a. Consider the sensitivity of the data, and statutory or other standards e.g. the HIPAA Privacy Rule for protected health information (PHI). See Section 3.2.1 Classify Data According to Level of Protection Needed.

b. See Chapter 3, Classifying and Protecting Data and IT Resources, for special instructions on providing access to department data by contractors and other agencies.

c. Document the approval and granting of access (such as who approved access, when, and why).

d. On an annual basis, such as at the time of the risk, threat, and vulnerability analysis (See Section 9.2.2 Annual Risk, Threat, and Vulnerability Analysis), review to determine if each user/group has authorized access to classified data necessary to meet the job requirements, and whether the level of access is appropriate for the job needs. Make corrections where needed.

e. Program areas must document and maintain their procedures for meeting the requirements of this standard.

S3. Managers must ensure that all servers connected to the network are fully secured, regardless of the confidentiality of data residing on the server. A poorly secured server can provide a backdoor entry/jumping off point for compromising other servers.

S4. Employees are held accountable for access to data and computer systems gained through the use of their user ID and password combination.

4.2.2 AUTHENTICATION REQUIREMENTS

Policy Statement 4.2.2

Adequate controls must be in place to authenticate users accessing department computers, networks, and applications; see DSHS IT Security References R4.2.2 Authentication Requirements, for further detail.

Standards

S1. Users and other entities such as applications or servers must be authenticated using such methods as login IDs and passwords, digital certificates, smart cards, or tokens.

4.2.3 USER IDS

4.2.3.1 General User ID Requirements

Policy Statement 4.2.3.1

Each system or application must have established procedures to ensure that each user ID is uniquely associated with a user.

Standards

S1. Electronic access to confidential information will always be protected, at a minimum, by a unique user ID, and a password that is constructed and protected as required by section 4.2.4 Use and Construction of Passwords.

S2. Assigning duplicate user IDs or sharing user IDs is prohibited, except that generic user IDs with limited access privileges may be used for:

Maintenance, troubleshooting, or system monitoring;

Training;

Shared workstations in secured areas, where no classified data is accessible unless all users have identical access needs; or

Program batch runs.

S3. Users shall not be assigned or be allowed to use bogus user IDs (a user ID created under a fictitious name). This does not prohibit the use of test user IDs.

S4. Access privileges associated with user IDs (for all computer systems) shall be suspended as follows:

a. Immediately for employees who are being terminated for cause,

b. Within five working days for employees who voluntary terminate employment with DSHS or who are transferred to another organization within DSHS, or

c. Within 30 calendar days for employees who remain within the unit but whose duties change. In such case, revoke only those privileges not required in the employee's new duties.

S5. User IDs shall be revoked/deleted as follows:

a. Within 10 working days after the employee terminates employment with the unit.

b. Within 120 days after access privileges have been suspended, but the employee has not transferred or terminated his or her employment with the unit. For mainframe systems, managers must request reinstatement of access privileges within this period to prevent deletion.

c. After a period of 180 days of inactivity. Alternatively, security administrators may use a semi-annual review cycle and delete any user ID that does not meet these criteria.

4.2.3.2 Construction of User IDs

The department has two standards for creating login IDs, the last name and initials format, and the RACF format (used primarily on the IBM mainframe.)

Policy Statement 4.2.3.2

Login ID standards must comply with one or both of the following two standards described below, except where noted.

Standards

S1. The preferred standard user ID format for Windows NT, Windows 2000, and the alias for the Exchange system will contain a maximum of eight characters and is constructed in the following order:

a. Up to the first five characters of last name, excluding spaces in compound names

b. First name initial

c. Middle name initial (if a middle name is used)

d. Tie breaker, if needed, in the following order:

(1) Numerical characters zero through nine (0 – 9)

(2) Alpha characters A - Z, excluding I and O

Exception: The variation of this format beginning with the first initial may continue to be used until it becomes feasible to convert to this standard. In addition, it is permissible to use the RACF format, described below, in lieu of this standard for other than RACF access.

S2. The standard format for RACF login IDs is constructed in the following order:

a. First two letters of last name

b. First two letters of first name

c. 300 (denotes agency code)

d. If necessary, use a tiebreaker in the fourth character. First try the employee's middle initial, or, if necessary, use 1-9.

4.2.4 USE AND CONSTRUCTION OF PASSWORDS

4.2.4.1 General Password Requirements

Policy Statement 4.2.4.1

Users and system administrators must be informed of the importance of constructing safe passwords and protecting them from unauthorized disclosure; see DSHS IT Security References R4.2.2 Authentication Requirements.

Standards

S1. Passwords are secret, and sharing your password with anyone else is prohibited, except for emergency access by your supervisor.

S2. Resist "social engineering," i.e. attempts by unauthorized persons to get a user to reveal a password or sensitive or confidential information, typically over the telephone.

S3. Change your password immediately following discovery that it has been compromised or shared in an emergency.

S4. Change passwords at least every 120 days or more often when required by the system. Where the feature is available, system administrators must configure systems to prompt users to change their passwords when they have expired.

S5. Do not store passwords on your computer for automatic entry in lieu of typing the password for initial log in.

S6. Do not write passwords down and leave them in a place where unauthorized persons might discover them. Also, do not store passwords in the same briefcase or suitcase as portable computers – especially those used to remotely access DSHS networks.

S7. Help Desk or LAN Administrator personnel must not reset a password without confirming the identity of the requesting party, and that the party has the authority to use the specified account.

S8. The initial password issued by the Help Desk or system administrator when resetting a password is valid only for the involved user's first log in session, at which time the password must be changed.

S9. System administrators/IT staff must ensure that default passwords are immediately changed when installing new software, etc.

S10. Where computer (CMOS) passwords are used, employees must ensure that supervisors have emergency access without compromising the passwords. This requirement can be met by using the "sealed envelope" technique, as follows:

a. Put your password in a sealed envelope, initial over the flap, and give it to your supervisor.

b. The supervisor must keep the envelope in a secured container and has responsibility to ensure that it is opened only for emergency purposes.

c. Anytime it is necessary for someone to open the envelope, they must notify you so that you can change your password.

S11. Where possible, password rules must be systematically enforced, including configuring systems so that:

a. Entry of passwords on the screen is not viewable (i.e. a character such as the * is used to hide the actual keyed entry.)

b. Passwords are encrypted during storage and transmission using at least 128-bit encryption.

c. A “lock-out” mechanism is activated after a maximum of up to five unsuccessful authentication attempts.

See DSHS IT Security Procedures P4.2.4.1.S10 Unsuccessful Login Attempts.

4.2.4.2 Constructing Passwords

Policy Statement 4.2.4.2

Users must adhere to the following requirements when constructing passwords; see DSHS IT Security Procedures P4.2.4.2 Constructing Passwords—Additional Suggestions, and DSHS IT Security References R4.2.4.2 Creating Strong Passwords for more information.

Standards

S1. Users accessing computer systems belonging to the federal government, other state or local agencies, and contracted mainframe services external to DSHS and DIS must construct passwords that comply with the password rules set forth by the owner of such systems.

S2. Passwords used on the UNISYS mainframe must be at least five characters in length, with a maximum of six characters.

S3. Passwords used for Windows NT systems and earlier versions of Windows, and other systems not specified in Standard **S4** below, must be constructed as follows:

a. Passwords must be a minimum of eight characters in length and contain at least one special character (either @, #, $) in the first seven characters.

b. Passwords must not contain your user name or any part of your full name.

S4. RACF and Windows 2000 passwords must be “hardened” in accordance with DIS standards, as follows:

a. Passwords must be a minimum of eight characters in length and must contain at least one special character (either @, #, $), one numeric character, and one alpha character. (Windows 2000 recognizes the difference between upper case letters and lower case letters. Using a combination of the two improves the security. RACF treats upper case and lower case the same.)

b. Passwords must not contain your user ID or any part of your full name.

c. Passwords may not be reused for five consecutive iterations.

S5. System administrators must use “hardened” passwords, where allowed, in all systems for administrative and services accounts.

S6. Passwords for user IDs associated with batch runs are an exception to the above rules as these passwords are set to a zero interval and never expire. Minimum or maximum lengths and composition are the same as above. (A batch user ID has no services authorized.)

Chapter 5: Network, Operating Systems, and Internet Security

5.1 INTRODUCTION

This chapter covers configuration and management of:

- Networked computers,
- Web server security,
- Operating systems, and
- Network devices, including connections to the Internet.

NOTE: The allowable uses of the Internet are covered in DSHS Administrative Policy 15.15, Electronic Messaging Systems and the Internet, and will not be duplicated here.

5.2 POLICIES, STANDARDS, AND GUIDELINES

5.2.1 WWW AND WEB BROWSER/WEB SERVER CONFIGURATION AND USE

The Internet/Intranet provides a number of services, of which the most common are e-mail, file transfer, and login from remote systems/clients.

5.2.1.1 Internet Use and Connectivity

Policy Statement 5.2.1.1

Internet use and connectivity must comply with the provisions of Administrative Policy 15.15 and the following standards.

Standards

S1. Use only the Washington State Department of Information Services (DIS) as the Internet service provider (ISP) for computers connected to the statewide area network (WAN.) This is for both economic and security reasons. DIS provides firewall filtering of traffic.

S2. Employees shall not establish an Internet connection (e.g. AOL, MSNetwork, etc.) to or from a networked station that bypasses the Washington State Department of Information Services (DIS) firewall. See Section 5.2.7 Wireless Networks and Devices, for details on wireless connectivity policies, standards, and guidelines.

Note: Commercial Internet service providers (e.g. AOL, MSNetwork, etc.) can be accessed through the DIS firewall.

S3. Do not provide a link between an external Internet connection and DSHS networks. Such links are created when privately owned computers or

LANs loaded with server software are connected to the Internet with a simultaneous connection to a department LAN via a dial-in or a direct line connection.

S4. Department personnel must not use state provided equipment or Internet connectivity to perform any illegal activities, e.g. deliberately spreading viruses, gaining unauthorized access to another computer, or making another network unusable by launching a denial of service attack.

S5. Department personnel must not:

a. Store department data on disk storage devices operated by vendors over the Internet; or

b. Link DSHS web sites to other Internet sites whose content may be in violation of the mission or policies of DSHS.

5.2.1.2 Minimum Web Client (Browser) Security Standards

Policy Statement 5.2.1.2

Web browsers must be selected, configured and operated in accordance with the following minimum-security standards; see DSHS IT Security Procedures P5.2.1.2-A Steps for Changing Your Options in Web Browsers, and DSHS IT Security Procedures P5.2.1.2-B MS "Quick Start" Instructions—Cross-Site Scripting.

Standards

S1. Department employees must use a supported version of either Internet Explorer or Netscape browsers. Excluding the specialized needs of the sight impaired, etc., the DSHS Chief Information Officer (CIO) must approve exceptions to this policy.

S2. All browser software must incorporate all security-related patches appropriate for the environment in which it is operating. See DSHS IT Security Procedures P5.2.3 Patch Management Process.

5.2.1.3 Web Server Security Standards

Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. Web server security includes the underlying operating system, the web server software, server scripts, and other associated components.

Policy Statement 5.2.1.3

Internet/Intranet web servers must be configured and managed securely.

Standards

S1. For Microsoft Internet Information Server, document the configuration using Microsoft's recommended Microsoft Internet Information Server 4.0 /(5.0) Security Checklist.

S2. Evaluate all vendor supplied upgrades, security bulletins, and patches; install those that are appropriate. See 5.2.3 Patch Management below.

S3. Users are forbidden to download, install or run web server software without prior approval of the organization's IT Manager.

S4. A public web server must not serve as a repository for confidential data. A public web server can act as a proxy for access to confidential data located on secure servers.

S5. All devices attached to the network, which allow user/administrator login, must be secured using login IDs and passwords (see Chapter 4, Access Security, Identification, and Authentication). Test environments, which are network attached, must have all applications and services secured as in the production environment.

S6. Configure and manage SQL/database servers in accordance with the standards described at DSHS IT Security References R5.2.2 Microsoft Tools.

5.2.2 OPERATING SYSTEMS FOR NETWORKS, SERVERS, AND WORKSTATIONS

Policy Statement 5.2.2

Computer operating systems must be configured and managed securely.

Standards

S1. System administrators must configure computers in accordance with the standards, as described at DSHS IT Security References R5.2.2 Microsoft Tools.

S2. System administrators must evaluate all vendor supplied upgrades, security bulletins, and patches. Those that are appropriate must be installed, to prevent exploitation by viruses, worms, or hackers. See 5.2.3 Patch Management below.

Guidelines

G1. Consider using Microsoft Baseline Security Analyzer for Microsoft-based systems, as described at DSHS IT Security References R5.2.2 Microsoft Tools.

5.2.3 PATCH MANAGEMENT

Policy Statement 5.2.3

The DSHS networked environment, and the SGN, must be protected by a comprehensive patch management process.

Standards

S1. All program areas will document and implement a patch management process, following the procedures detailed at DSHS IT Security Procedures P5.2.3 Patch Management Process.

S2. When necessary, the DSHS IT Security Administrator may be required to authorize blocking or disconnection of infected machines or segments. If initiated, this state will be maintained until the impacted program area has reported the machine(s) or segment as having been patched and cleaned.

5.2.4 NETWORK DEVICES AND FIREWALLS

Policy Statement 5.2.4

Network devices, such as routers, hubs, switches, and firewalls must be configured and managed securely.

For more information see DSHS IT Security References R5.2.4 Network Devices and Firewalls.

Standards

S1. Minimize the risk of "back doors" by identifying and changing default passwords and account names. Passwords must conform to the standards in Chapter 4, Access Security, Identification, and Authentication.

S2. Limit telnet and/or TFTP (Trivial File Transfer Protocol) access to routers, hubs, and switches.

S3. Prevent the unauthorized collection of configuration information by using Access Control Lists (ACL) to limit what ports may be accessed.

S4. Where feasible, disable any Routing Information Protocol version 1 (RIPv1) capability on routers; and/or disable any RIP packets at border routers.

S5. ISSD Network Services will administer all firewalls used to protect individual DSHS networks (WAN and LANs) from the DIS backbone network. Note: This does not include firewalls for wireless segments, which must be maintained by the responsible program area.

5.2.5 REMOTE ACCESS

5.2.5.1 Dial Access Software

Policy Statement 5.2.5.1

Dial access software must be configured for optimum protection of department information.

Standards

S1. The use of passwords is mandatory.

S2. Do not connect a modem to an individual workstation. If remote control software such as LapLink, Carbon Copy, or PC Anywhere is needed, use the Department's centralized Virtual Private Network (VPN), Shiva, or remote dial access service, both of which are administered by ISSD, to connect to the workstation.

S3. LAN system administrators who choose to activate LAN-based Remote Access Service (RAS) must configure RAS to take advantage of the security features offered by the software.

S4. Where possible, implement the days of the week and the time of day feature to control remote dial-in connections to the host.

5.2.5.2 Remote Systems

Policy Statement 5.2.5.2

Systems used for remote access must be protected in a manner similar to DSHS desktop/laptop systems

Standards

S1. Access to DSHS systems must be controlled, at a minimum, by passwords.

S2. All systems used for remote access must have current anti-virus software installed and maintained.

S3. Operating system and applications (such as Office Suite) must have security patches kept current.

S4. Confidential information must not be stored on home computers.

Guidelines

G1. Procedures for patch management (see DSHS IT Security Procedures P5.2.3 Patch Management) should be followed by home users. Applying the patches is mandatory, and the process for assessment and testing are recommended.

5.2.6 ANTI-VIRUS SOFTWARE MEASURES

5.2.6.1 Anti-Virus Software

Policy Statement 5.2.6.1

Anti-virus software must be installed and used in such a way as to minimize the risk of viral infection to department networks and workstations.

Standards

S1. System administrators must install anti-virus software on all computers (excluding mainframes), and configure it to:

a. Periodically scan all files on the computer, and

b. Automatically scan all new files introduced to the computer.

S2. E-mail administrators must install anti-virus software on all e-mail servers and gateways to scan for viruses contained in e-mail messages.

S3. System administrators must ensure that anti-virus software is kept current. New definition files must be loaded as soon as possible after they are released.

S4. Users must consult system administrators if there is a need to temporarily disable anti-virus software.

Guidelines

G1. All DSHS organizations are strongly encouraged to use, on all computers, the Network Association, Inc. (NAI) anti-virus software for which the department has purchased a site license. This anti-virus software is free to all departmental organizations.

5.2.6.2 Other Precautions

Policy Statement 5.2.6.2

System administrators and users must take reasonable precautions to prevent virus infection.

Standards

S1. Users must not download, open, execute, or install any software, "shareware", public domain programs, or executable files unless approved by the system administrator, and then not until they have been checked for viruses by divisional or local IT staff.

5.2.6.3 Responding To Virus Incidents

Policy Statement 5.2.6.3

ISSD and divisional/local IT staff must respond swiftly and decisively at the first indication of a virus outbreak to control it's spread within the department.

Standards

S1. Any user who suspects they may have a virus on their computer shall immediately report it to their IT support person.

S2. All instances of virus infection must be immediately reported to the ISSD Exchange Administrator.

5.2.7 WIRELESS NETWORKS AND DEVICES

The introduction of wireless as an alternative method to access the DSHS Wide Area Network (WAN) imposes new risks associated with unintended access and/or disclosure of data not only to the DSHS WAN, and Local Area Networks (LANs), but also the risk of potential exposure to the entire State Government Network (SGN).

Policy Statement 5.2.7

Wired networks must be protected from wireless networks.

Standards

S1. When implementing 802.11x wireless LAN access to DSHS computing resources:

a. Establish and document wireless access security practices.

b. Firewall all wireless access point connections from your LAN and the DSHS WAN (see DSHS IT Security Procedures P5.2.7.S1 Wireless Networks and Devices).

c. Use industry standard authentication and encryption methods (i.e. strong passwords and a VPN or SSL type encryption; WEP encryption is not secure).

d. Administrations will perform a self-audit on a regular basis to locate any rogue wireless devices. In addition, assessment will be incorporated into the IT Security Audits conducted every two years (See Section 9.2.3 Biennial IT Security Audit Program).

S2. All wireless devices using CDPD (Cellular Digital Packet Data) connection must have Internet activation and access coordinated through ISSD, Office of Communications (Network Services).

Chapter 6: System Design, Development, Maintenance, and Operations

6.1 INTRODUCTION

This chapter covers IT security requirements for:

- Systems design and development,
- System maintenance, and
- Operation of production computer applications and systems.

Security is an important consideration in this process, and the level of security required should be commensurate with the sensitivity of the data being processed and the requirements of applicable federal and state laws and regulations.

6.2 POLICIES AND STANDARDS

6.2.1 SECURITY REQUIREMENTS DURING DESIGN AND DEVELOPMENT

Policy Statement 6.2.1

IT security must be an integral part of the system development or acquisition process. See DSHS IT Security Procedures P6.2.1 Internet Based Applications, for details.

NOTE: Failure to address and specify security requirements early in a project increases the likelihood that security will prove to be inadequate or that additional costs will be incurred.

Standards

S1. Staff will:

a. Identify the category of data (see Chapter 3, Classifying and Protecting Data and IT Resources) to be processed or accessed by the system.

b. Ensure that appropriate IT security measures are included in the design of the system from the beginning of the project, and

c. That plans for securing the system are included in the system's documentation.

S2. Where audit trails recording access to information are required, managers or developers must design applications such that the audit trails will be secure, and easily maintained and reconstructed.

S3. All program code shall be reviewed for security considerations, including:

a. Security measures that are written into the application;

b. Elimination of potential backdoors; and

c. Poorly coded fiscal checks and balances to preclude possible fraud.

The person reviewing the code for fiscal applications must be someone other than the person who wrote the code and, where possible, should be a DSHS employee.

S4. For Internet-accessible applications:

a. All applications accessed from the Internet must pass through the State Fortress environment, managed by the Department of Information Services. Requests to establish access through Fortress are managed by the Office of Communications, ISSD.

b. Use the following methods to validate user input:

(1) Use code running on the server (as opposed to the client computer) to validate all user input. Code running on the client computer may also validate input data, but should not be relied on (because client code can be bypassed).

(2) Use a validation process that identifies a set of safe characters or character combinations to accept, and rejects all other input.

(3) Use stored procedures or parameterized queries to generate SQL query code.

c. Prevent buffer overflows by either of the following means:

(1) Use managed code languages such as Visual Basic.NET, C#.NET, or Java that automatically provide bounds checking; or

(2) Scrutinize any use of non-managed code languages such as C or C++, or of untested DLLs or other components, to ensure that bounds checking or data-size checking is done.

d. Contact ISSD's IT Security Unit early in the design process to arrange for a review of the application by the department's Internet Applications Security Review Team (see Section 9.2.9 Internet Web Site Security Reviews).

S5. Developers must design applications that are compatible with available standard security facilities and use common practices rather than create unique methods. Examples of standard facilities include:

a. RACF access control for the IBM environment; TIP security for the Unisys environment

b. The Security Account Manager program for the Windows NT environment

c. Fortress or Transact Washington for accessing applications available over the Internet

Exceptions must be approved in writing by the DSHS Chief Information Officer (CIO) for Internet applications that do not meet this criteria.

S6. Developers must protect non-database files residing on the UNISYS mainframe(s) with read and write protection using Access Control Records (ACR).

S7. Developers must deploy file transfer utilities with appropriate security features for the transfer of files between computing systems.

S8. System specifications must be set so that the integrity of data is maintained at all times.

6.2.2 SECURITY REQUIREMENTS DURING MAINTENANCE

Policy Statement 6.2.2

Departmental security requirements must be met during systems maintenance.

Standards

S1. All software applications maintenance activities must comply with the applicable provisions of this manual.

S2. All changes in production applications and systems must be documented and approved in writing by the appropriate IT Manager.

S3. Restrict access to source code and program documentation only to authorized employees on a need-to-know basis for programs that process classified data.

6.2.3 APPLICATION ACCESS AND PRIVILEGES

Policy Statement 6.2.3

Access privileges for each employee must be controlled to ensure that the employee can only access those applications and processes needed in the performance of his or her duties.

Standards

S1. Operations Managers must require all applications on DSHS mainframe or client server systems to be regulated by standard access control systems software such as RACF, SIMAN and Security Option 1 for the UNISYS, or SAM for Windows.

NOTE: Access control systems software can be:

a. A feature of an operating system
b. An add-on access control package
c. A front-end or firewall that performs access control

S2. A user's session must initially be controlled by access control systems software, and, if defined permissions allow it, control will then be passed to separate application software.

S3. Managers of mainframe operations must ensure that operators are limited to only those system options for which they have privileges.

S4. Managers of mainframe operations must separate work duties and responsibilities of employees in the data control center, including input/output processing, production control, and operations.

S5. No modifications by operations staff to production data, production programs, or the operating system are permitted.

S6. Only authorized maintenance personnel may access the production library. Controls must be in place to prevent unauthorized use or removal of tape files, diskettes, and other media.

6.2.4 MODIFYING MAINFRAME PRODUCTION SYSTEMS

Policy Statement 6.2.4

Managers of operations must employ a formal change control procedure to ensure only authorized changes are made to computer production processing at DSHS.

Standards

S1. Establish and document a system change control procedure.

S2. Requests for changes to production programs or systems shall be in writing. This may be done by e-mail so long as the recipient of the request confirms its authenticity, e.g. by phone.

S3. Provide operations staff with adequate training and operating documentation before a system is moved into production processing.

6.2.5 LOGS

Policy Statement 6.2.5

Managers of IT operations must require logs to be maintained for DSHS production application systems.

Standards

S1. All computer systems running DSHS production application systems must include logs which record:

a. Changes to critical application system files

b. Additions and changes to the privileges of users

c. System start-ups and shutdowns

d. Attempted system access violations

S2. It must be possible to reconstruct activities from operation logs.

S3. Logs must be secured to prevent modification, and must be accessible only by authorized persons.

S4. Production systems servers connected to the Internet are to have system logs maintained on Write Once Read Many (WORM) storage media or similar technology. This will help preserve reliable logs that could be admissible in a court of law.

S5. Logs must be retained for a minimum of three years.

Chapter 7: Electronic Messaging Systems

7.1 INTRODUCTION

This chapter covers:

- The use of electronic messaging systems, and
- The management and retention of information transmitted by, and stored in, electronic messaging systems.

NOTE: An Electronic Messaging System is any system that transmits and/or stores voice or typed communication/recordings. These messaging systems are commonly referred to as the phone (with voice mail) and e-mail respectively.

7.2 POLICIES AND STANDARDS

NOTE: See Chapter 5, Network and Operating Systems Security, for anti-virus software requirements.

7.2.1 E-MAIL

This Section augments the provisions of Administrative Policy 15.15, Use of Electronic Messaging Systems and The Internet, which provide extensive coverage of this subject. Topics covered by 15.15 include:

- Employee use of electronic messaging systems and the Internet
- Public records, disclosure and retention (as it pertains to electronic messaging)
- Confidential Information (protection)
- Electronic backups and storage
- Distribution lists
- User Information
- System monitoring
- Recurring Internet policy messages

7.2.1.1 Allowable Uses of E-Mail

Policy Statement 7.2.1.1

E-mail, including e-mail over the Internet, shall be used only for those purposes allowed by state regulations and department policy.

Standards

S1. Department personnel must not use state provided equipment or e-mail connectivity to perform any illegal activities, e.g. deliberately spreading viruses, gaining unauthorized access to another computer, or making another network unusable by launching a denial of service attack.

S2. Electronic messaging systems may not be used to establish agency policy. Electronic messaging systems may be used for immediate dissemination of such executive level messages, but must not replace other policy dissemination mechanisms. One reason for this is to keep from having to archive e-mail messages for long periods of time. See also Administrative Policy 11.07.P.

7.2.1.2 Backup and storage for e-mail

Policy Statement 7.2.1.2

Establish procedures to ensure that e-mail messages are retained or deleted in accordance with state regulations and department policy.

Standards

S1. System administrators of electronic messaging systems shall have scheduled backup procedures, retention schedules, and off site storage of backups, as described at Chapter 3, Classifying and Protecting Data and IT Resources.

S2. Employees shall delete from electronic storage informational messages such as meeting notices, reminders, informational notes, and telephone messages once the administrative purpose is served.

S3. E-mail retention is the responsibility of the sender and receiver of the message, not the backup process. Back-up copies performed by ISSD staff are retained for 21 days and are not used for records retention purposes. The centralized backup of e-mail is for disaster recovery purposes only.

Guidelines

G1. Each program area should determine their preferred method of retention. Some suggested methods are printing, following regular retention processes for the hardcopy, and electronic storage in personal archive folders.

7.2.1.3 Exchange E-Mail Administrator Program

The Exchange Administrator program allows ISSD to delegate to divisional Exchange administrators the ability to administer their organizations' e-mail accounts.

Policy Statement 7.2.1.3

The Microsoft Exchange Administrator program must be configured securely.

Standards

S1. Divisional Exchange administrators will only install the Exchange Administrator program on highly secure computer systems.

S2. The operating system must be Microsoft Windows NT Server, 2000 Server, NT Workstation, 2000 Professional Workstation, or Microsoft Windows XP Professional.

S3. The system must not be remotely accessible from outside of the DSHS Network, i.e., access should not pass through or around a firewall (no dial-in).

S4. The system must not have asynchronous communication capabilities, e.g. RRAS, RAS, Shiva, or Citrix Winframe/Metaframe.

S5. Install Network Associates Anti-Virus, or equivalent, software on the system, and enable the "System Scan", "Download Scan" & "Internet Filter" features.

7.2.2 VOICE COMMUNICATIONS

See DSHS IT Security Procedures P7.2.2 Protecting Voice Mail Access and Data, for more information.

7.2.2.1 Protecting Long Distance And Voice Mail Access Codes

Policy Statement 7.2.2.1

Staff must keep long distance (SCAN or other carriers) and voice mail access codes confidential.

Standards

S1. Access codes are confidential and must not be:

a. Shared with others, or

b. Written or posted where they are easily seen.

S2. Managers must request cancellation and re-issue of a SCAN access code that has been compromised.

S3. The person to whom the telephone number is assigned must change a voice Mail access code that has been compromised.

S4. Telecom coordinators must ensure voice mailboxes are set-up (initialized) within two weeks of installation. If a voice mailbox has been un-initialized for more than thirty days, it must be deleted.

7.2.2.2 Cellular Telephone Security

Policy Statement 7.2.2.2

Establish procedures to ensure cellular telephone access is secure.

Standards

S1. Employees will keep cellular telephones in safe storage when not in use.

S2. When a cellular phone is stolen or lost, immediately report it in accordance with DSHS IT Security Procedures P10.2.2 Reporting Suspected Incidents. Take other appropriate action such as disconnecting or freezing the number, or transferring the service to a new set.

S3. If cellular phones are to be used for confidential information, use digital phones that encrypt transmissions.

Guidelines

G1. It is preferable that employees use digital cellular phones that encrypt transmissions. Note that the digital phones available under state contract encrypt transmitted information to prevent "cloning" (capture of the codes used to make calls and applying them to an unauthorized instrument).

G2. Turn off analog cellular phones when not in use to avoid cloning. This is especially true in densely populated areas or near airports. Alternatively, employees should consider using a pager in conjunction with an analog cellular phone. Then employees can be called on their beepers, and make return calls on their cellular phones.

7.2.2.3 Telephone And Voice Mail System Physical Security

Policy Statement 7.2.2.3

Keep telephone and voice mail system hardware in a secured room.

Standards

S1. Telephone system and voice mail system hardware must be placed in a locked room. Unused telephone equipment must be secured until needed.

7.2.2.4 Telephone And Voice Mail System Electronic Access Security

Policy Statement 7.2.2.4

Telecom coordinators will ensure that only authorized persons have electronic access to telephone and voice mail systems.

Standards

S1. Telecom coordinators will ensure that telephone and voice mail system passwords are kept in a secure place.

S2. Telecom coordinators will ensure that remote access for telephone switch systems and for voice mail systems is configured to dial back to authorized phone numbers, where technically possible.

7.2.2.5 Monitoring Calls/Use Of Speakerphones

Policy Statement 7.2.2.5

If a call is monitored, recorded, or played on a speakerphone, all parties to the call must be notified.

Standards

S1. Before you begin monitoring, recording a call, or playing it on a speakerphone, notify all parties to the call, and let them know who is listening.

Chapter 8: Encryption and Data Integrity

8.1 INTRODUCTION

A. This chapter covers policies, standards and guidelines for securing data through the use of encryption and data integrity tools.

1. Encryption is the process of scrambling data to make it unreadable except by the intended recipient(s), usually by employing symmetric and asymmetric algorithms.
2. As used here, data integrity ensures that data has not been altered during transit over unsecured media such as the Internet and is usually provided by message authentication codes or hash values.

B. Greater detail is available in the DSHS IT Security References R8.1 Encryption Information Sites.

8.2 POLICIES, STANDARDS, AND GUIDELINES

8.2.1 DATA ENCRYPTION

Policy Statement 8.2.1

Implement encryption techniques to prevent unauthorized access to classified department data as specified in the following standards.

Standards

S1. Classified data transmitted through the Internet or Intergovernmental Network (IGN) must be encrypted using minimum key sizes of 128 bits for symmetric keys, and 1024 bits for asymmetric keys.

NOTE: This standard applies to all outgoing and incoming classified data, except data sent by clients, whether the data originates from a Web, SQL, FTP, E-mail, or other site.

NOTE: Tools available to implement this requirement are described at DSHS IT Security References, R8.2.1 Cryptographic/Integrity Methodologies and Tools.

See also DSHS IT Security Procedures P8.2.1.S1 Encryption of Special Handling Information

S2. Secure e-mail: Use the department's Integrated Message Exchange (IME) system when e-mail messages and/or attachments transmitted through the Internet or Intergovernmental Network (IGN) must be encrypted.

S3. Secure file transfer: When secure exchange of information from one application or user to another is needed, it must meet the following criteria:

a. All manipulations of data during the exchange are secure.

b. If intercepted during transmission, data cannot be understood.

c. The intended recipient is the only one who can understand the transmitted information.

d. Confirmation is received that the intended recipient received the data.

S4. Encrypted storage of data: When encrypted storage of data is needed, it must meet the following criteria:

a. Encrypt data using a minimum key size of 128 bits for symmetric keys.

b. Maintain the ability to un-encrypt stored data using an authorized process, and through a pre-defined recovery period identified by the organization.

c. Protect the encryption and decryption method (key and algorithm).

8.2.2 DATA INTEGRITY

Policy Statement 8.2.2

Implement electronic mechanisms to ensure that there is no unauthorized alteration or deletion of electronic protected health information (EPHI), as specified in the following standards.

Standards

S1. For EPHI transmitted through the Internet or Intergovernmental Network (IGN), a hash value will be computed by both sender and recipient in order to ensure that EPHI has not been altered.

NOTE: Tools available to implement this requirement are described at DSHS IT Security References, R8.2.1: Cryptographic/Integrity Methodologies and Tools.

8.2.3 DIGITAL CERTIFICATES

A. Digital certificates provide a means of managing public key pairs by binding the public key of the pair to an individual or machine (the private key is never identified by certificate). PKI-related software (encryption, authentication, digital signatures, etc) uses the associated key pair to perform a particular function. (It is important to understand that the certificate itself does not perform any of these functions, such as encrypting or signing documents).

B. The DIS Master Contract established with Digital Signature Trust (DST) provides economy of scale and a standard for obtaining digital certificates. In addition, the voucher system established to track this process allows certificate management and report generation.

Policy Statement 8.2.3

The following standards apply to all digital certificates used within DSHS.

Standards

S1. Use the DIS Master Contract with DST to procure digital certificates, unless granted an exception by the DSHS Chief Information Officer (CIO).

S2. The DSHS CIO will appoint a Certificate Coordinator (CC) in the ISSD IT Security Section to facilitate the purchase and use of digital certificates in DSHS.

S3. Use the DST/ISSD voucher system for purchasing certificates, and coordinate all purchases through the DSHS certificate coordinator. As part of the voucher process, the names of the digital certificate users (or server name, in the case of server certificates) must be identified before vouchers can be issued.

S4. The private key for certificates whose associated key pair is used for encryption and decryption of data must be escrowed to ensure no data is lost due to key loss or corruption.

S5. The private key for certificates whose associated key pair is used for signing documents (digital signatures) is never escrowed, since the private key must remain secret and under the direct control of the signing authority. Accordingly, separate public key pairs must be used for encrypting and signing documents.

S6. Private keys stored on a hard drive must be encrypted.

S7. The department must have a procedure for revoking certificates, including certificates purchased by the department for clients and business partners. Certificates may be revoked either by the person to whom the certificate was issued, or by the DSHS certificate coordinator at the request of executive-level management in the organization that approved the purchase of the certificate.

Guidelines

G1. ISSD (both IT Security and Network Services) offers consultative services for deciding when, where, and how to use certificates, including what assurance levels to use.

8.2.4 TOKENS

A. Security tokens include Smartcards, time-synchronized tokens, and challenge-response tokens.
   1. Smartcards (including digital certificate fobs) frequently provide at least the key activation and signing components of cryptographic services, and they may provide other cryptographic services as well.
   2. Time-synchronized and challenge-response tokens only provide authentication functionality, and will typically be integrated into the PKI Architecture through modifications to the system security-enabling services (particularly the logon and obtain credentials components of those services).

B. Tokens are the highest level of security short of biometrics (the use of biologically unique data, such as retinal scan, thumb print, etc., to identify a user).

Policy Statement 8.2.4

Managers must evaluate the need for tokens on a case-by-case basis, and authorize their use where the business need (such as flexibility) or enhanced security justifies the additional cost, or federal or state regulations dictate their use. If tokens are used, the following standards apply:

Standards

S1. Report all lost or stolen tokens immediately to program area management and to ISSD IT Security.

S2. Since the loss of a token potentially compromises the private key, the compromised digital certificate must be revoked immediately, either by the individual to whom the certificate was issued, or by the ISSD Certificate Coordinator.

Chapter 9: Security Assessments, Reviews & Reports

9.1 INTRODUCTION

This chapter provides standards and guidelines for security-related assessments, reviews, and reports.

9.2 POLICIES AND STANDARDS

9.2.1 USING AUTOMATED SECURITY ASSESSMENT TOOLS

Policy Statement 9.2.1

Limit the use of software (automated assessment tools) designed to test for vulnerabilities in networks and servers according to the following standards.

Standards

S1. Managers may authorize the use of automated security assessment tools to test for vulnerabilities within their own networks. The use of these tools to probe other networks is strictly prohibited.

S2. The ISSD Internet Applications Security Review Team will use automated security assessment tools when conducting the formal reviews of Internet applications.

9.2.2 RISK, THREAT, AND VULNERABILITY ANALYSES

Policy Statement 9.2.2

Risk, threat, and vulnerability analyses will be conducted annually to help identify the department's principal IT security exposures.

Standards

S1. DSHS organizations shall participate in the department's annual risk assessment and self-evaluation (RASE) process, which is administered by the DSHS Internal Control Officer (see Administrative Policy 16.05)

a. The DSHS IT Security Administrator shall provide the DSHS Internal Control Officer an annual update to that part of the RASE checklist that addresses IT security.

b. The IT Security part of the RASE process will be designed to meet the requirement for annual updates to risk, threat, and vulnerability analyses.

S2. Risk, threat, and vulnerability analyses shall:

a. Be accurate and thorough;

b. Address the confidentiality, integrity, and availability of data and systems;

c. Be updated annually or whenever there are changes in systems, operations, or environments that significantly affect security.

S3. Documentation of risk, threat, and vulnerability analyses shall be retained for 6 years, and made available to those persons responsible for acting on the information contained therein.

S4. The completed section of the annual RASE checklist, relating to IT security, shall be submitted to the DSHS IT Security Administrator by May 31st of each year.

S5. The DSHS IT Security Administrator shall review assessments to ascertain any needed improvements in IT security policies.

9.2.3 BIENNIAL IT SECURITY AUDIT PROGRAM

Federal regulations 45 CFR 95 and 7 CFR 277 both require biennial IT security audits. The HIPAA Security Rule, 45 CFR 164.308(a)(8), requires periodic evaluations. In addition, DIS policy requires an IT security audit every three years. (See the DSHS IT Security References R9.2.3 DIS IT Security Policy—Audit Requirement).

Policy Statement 9.2.3

The DSHS Chief Information Officer (CIO) will establish and oversee the Department's IT Security audit program for complying with federal and state IT security audit requirements.

Standards

S1. ISSD shall contract with the State Auditor's Office (SAO) to perform the mandatory biennial IT security audits.

S2. The DSHS IT Security Administrator, in coordination with Division directors/designees, must schedule biennial audits.

S3. The SAO must conduct the audits using instructions provided by the DSHS IT Security Administrator. These instructions must reflect department policy governing IT security.

S4. Auditors may examine all DSHS computer systems, and the computers of all users including department-owned computers residing in an employee's home, if deemed necessary.

S5. The SAO must provide audit results electronically to the DSHS IT Security Administrator, who will coordinate corrective actions with the applicable departmental organization.

S6. Where audit results are in question, the DSHS IT Security Administrator must make a concerted effort to resolve issues informally. If this process fails, managers may appeal audit results to the DSHS CIO.

S7. DSHS IT Security must retain an electronic copy of audit results on file for five years.

9.2.4 INSPECTION PROCEDURES FOR SAFEGUARDING IRS TAX INFORMATION

DSHS is required by IRS Publication 1075 to conduct periodic inspections during the year to ensure that safeguards for protecting IRS tax information are adequate. The department satisfies this requirement using internal professional auditing staff to perform an annual audit of the department's compliance with the provisions of the DSHS IT Security Manual (details Chapter 11) and IRS Publication 1075.

Policy Statement 9.2.4

The DSHS CIO has responsibility for ensuring that annual internal inspections are conducted to satisfy the requirements of IRS Publication 1075.

Standards

S1. The conduct of internal inspections will be divided between the DSHS Office of Operations Review and Consultation (OORC) and the DCS Program Review section, as follows:

a. The DSHS Office of Operations Review and Consultation (OORC) must audit:

- DEAP Headquarters QC
- DEAP QC field units
- ISSD Operations and ISSD IT Security
- Mainframe computer procedures for both DEAP and DCS

b. The DCS Program Review section (self-assessment staff) must audit the applicable DCS headquarters and field office program functions.

S2. OORC must provide the DSHS IT Security Administrator with a copy of the audit results by July 1 of each year. These findings will be forwarded to the appropriate division for corrective actions. Actions taken to correct noted deficiencies must be documented and returned to the DSHS IT Security Administrator by August 15 for inclusion in the upcoming annual Safeguard Activity Reports to the IRS.

S3. The DCS self-assessment staff must take responsibility for ensuring corrective actions are taken for deficiencies noted in their review. A copy of both the audit results and the corrective actions taken must be forwarded to the DSHS IT Security Administrator by December 15 for inclusion in the upcoming annual Safeguard Activity Reports to the IRS.

S4. The DSHS IT Security section must maintain a copy of audit findings and responses for the current year and three previous years. The copy included in the Safeguard Activity Reports will meet this requirement.

9.2.5 IT SECURITY AUDITS OF DSHS BY THE IRS

The IRS performs two separate audits of DSHS procedures for safeguarding IRS tax information every three years. One audit covers the Income Eligibility and Verification System (IEVS) cross-match process administered by DEAP, and the second audit covers DCS procedures for safeguarding tax information received as part of the Tax Refund Off-set Program from the Office of Child Support Enforcement (OCSE) in Washington, D.C.

Policy Statement 9.2.5

Section 2.4, IRS Publication 1075, requires that the department centralize safeguard responsibility and establish and maintain uniform safeguard standards for protecting federal tax information. This centralized role is performed by the DSHS IT Security Administrator on behalf of the DSHS CIO.

Standards

S1. Both DCS and DEAP must immediately notify the DSHS IT Security Administrator as soon as they become aware of an impending audit by the IRS. In addition, the DSHS IT Security Administrator must be included in the kickoff meeting and any other meeting where:

a. Policy is an issue; or

b. Areas outside of the respective division are being reviewed, including ISSD Operations and DIS.

9.2.6 IT SECURITY AUDITS OF DSHS BY OTHER FEDERAL AGENCIES

Periodically, the department is audited for IT security by other federal agencies, including the Social Security Administration (SSA). In addition, the Department of Health and Human Services (DHHS) contracts with the Washington State Auditor's Office (SAO) to perform Medicaid audits, which include IT security functions.

Policy Statement 9.2.6

The IT Security Section will participate in security audits by federal agencies to explain and/or defend IT security policies for the department as required during such audits.

Standards

S1. Divisions must immediately notify the DSHS IT Security Administrator as soon as they become aware of an impending audit by the SSA, DHHS, etc., where IT security will be an area of interest to the auditors. In addition, the DSHS IT Security Administrator must be included in the kickoff meeting for such audits.

9.2.7 DSHS ANNUAL CERTIFICATION TO THE ISB

Policy Statement 9.2.7

The Department Secretary must certify annually to the Information Services Board (ISB) that an IT Security Program has been developed, implemented and tested in accordance with DIS policies and standards.

Standards

S1. The IT Security Section must prepare an annual IT Security certification letter to be signed by the DSHS Secretary or designee. This letter is due to the ISB by June 30 of each year.

9.2.8 ANNUAL SAFEGUARD ACTIVITY REPORTS

Policy Statement 9.2.8

The DSHS CIO is responsible for the preparation and submission of the annual Safeguard Activity Reports for DCS and DEAP as required by IRS Publication 1075.

Standards

S1. Safeguard Activity Reports must be prepared in accordance with specifications set forth in IRS Publication 1075. The DSHS CIO must sign the reports for the Secretary.

S2. The report prepared for DEAP is due to the IRS Office of Disclosure on or before September 30 of each year, and the report prepared for DCS is due to the same office by January 31 of each year.

S3. A copy of each Safeguard Activity Report must be retained on file by ISSD for the current year and three previous years.

9.2.9 INTERNET WEB SITE SECURITY REVIEWS

Policy Statement 9.2.9

Reviews of Internet applications and web sites will be conducted.

Standards

S1. DSHS organizations that are developing an application or web site that will be accessible from the Internet will contact ISSD early in the design process to arrange for a review of the application and/or supporting systems by the department's Internet Applications Security Review Team. For more information, see the IT Security Review Methodology document. **[[LINK TO http://techzone.dshs.wa.gov/IT_Services/Support___Consultation/securityiasrt.stm]]**

Chapter 10: Detecting, Investigating, and Reporting IT Security-Related Incidents

10.1 INTRODUCTION

This chapter describes the department's policies for detecting, investigating, and reporting suspected IT-related security incidents.

10.2 POLICIES AND STANDARDS

10.2.1 DETECTION

Policy Statement 10.2.1

Establish procedures for detecting unauthorized access or attempted access to IT resources or data. If this process must be implemented in stages (due to funding, etc.) detail the stages, and anticipated milestones.

Standards

S1. System administrators must monitor systems for indications of unauthorized access or access attempts. This must include regularly reviewing records (weekly, at a minimum) of information system activity, such as audit logs or access reports.

Guidelines

G1. Automated tools may facilitate this process of review, to include pointing out odd entries, reporting cumulative data, and notifying by pager/email when events occur. There are other tools which may be used to provide an increased level of monitoring of system activity.

G2. Depending on the critical or confidential nature of the system or data, the logs should be monitored on a daily basis. If the system is less critical, or there is reduced or no confidential data, then the monitoring can be less frequent, but must be reviewed at least weekly.

10.2.2 INVESTIGATING IT SECURITY-RELATED INCIDENTS

Policy Statement 10.2.2

Investigate and report all instances of suspected IT related theft, fraud, and misuse of resources.

Standards

S1. Whenever evidence clearly shows that there has been a significant IT related theft, fraud, misuse of resources, or breach of security, an investigation must be performed. The objectives of this investigation will be to:

a. Determine how the incident occurred;

b. Determine responsibility;

c. Facilitate measures to prevent recurrence.

S2. Immediately report suspected incidents to the DSHS IT Security Administrator, in accordance with DSHS IT Security Procedures P10.2.2.S2 Reporting Suspected Incidents.

S3. Obtain and safeguard evidence relating to incidents involving misuse or unauthorized access.

S4. During an investigation, protect the confidentiality of information gathered. See DSHS IT Security Procedures P10.2.2.S4 Securing and Protecting Evidence, for further detail.

10.2.3 ELECTRONIC MONITORING OF USERS

Policy Statement 10.2.3

Ensure that appropriate safeguards are observed whenever users' actions or data are electronically monitored or accessed.

Standards

S1. System administrators may be authorized to engage in monitoring activities as follows:

a. For an authorized training program, planned application design, or for network troubleshooting procedures, provided that affected employees are first notified, or

b. For a properly authorized investigation, when approved in writing by executive management.

System administrators will not access users' messages or files except as provided in standard **S4**, below (see also Administrative Policy 15.15.G).

S2. Use a log-on warning banner or similar message to warn uninvited users who are logging on remotely that their use of the system is not allowed, and that their use of the system may be monitored. See sample language for warning banners at DSHS IT Security Procedures P10.2.3.S2 Warning Banners-Sample.

NOTE: The U.S. Department of Justice recommends the use of a warning banner so that any evidence that may be collected of illegal activity will be admissible in court.

S3. ISSD will monitor Internet use and will provide the results to program directors for disposition as deemed appropriate.

S4. Messages and files residing on department systems are state property and subject to access by an employee's supervisor. For details, see Administrative Policy 15.15.G, Use of Electronic Messaging Systems and

the Internet, and DSHS IT Security Procedures P10.2.3.S4 Accessing Employee's Files.

Chapter 11: Safeguarding Federal Information

11.1 OVERVIEW

A. DSHS receives two types of federal data that require safeguard measures exceeding normal client-confidentiality requirements:

- Social Security Administration (SSA) information, and
- Internal Revenue Service (IRS) tax information.

See DSHS IT Security References R11.1 Safeguarding Federal Information.

B. The provisions of this chapter pertain to all department organizational units that process or use SSA or IRS tax information.

11.2 POLICIES AND STANDARDS FOR SAFEGUARDING SSA INFORMATION

The Social Security Administration requires stringent safeguards for protecting SSA information. The following standards augment other standards in this manual to comply with SSA requirements as set forth in the Social Security Administration's Online Data Exchange manual.

11.2.1 REQUIREMENTS FOR SAFEGUARDING SSA INFORMATION

Policy Statement 11.2.1

All employees must comply with the special requirements, contained in the standards below, for safeguarding SSA information.

Standards

S1. All employees who have access to SSA information must receive an initial briefing and annual refresher briefings regarding the confidentiality of SSA data and the associated penalties for unauthorized disclosure. Form DSHS 16-156, Statement of Understanding, is available for this purpose.

Maintain records of employee briefings for six years.

S2. SSA Information may be viewed and used only for purposes directly related to administration of the Food Stamp, Title IV-A, Title XIX Medicaid, State Medical and General Assistance, and other needs based programs. Any personal use of SSA Information is strictly prohibited.

S3. Access to SSA Information must be limited to individuals whose duties specifically require access in the performance of their assigned duties.

S4. File documents containing SSA client information in a secure place after use.

S5. The department shall keep an automated audit trail of all access to SSA information, as follows:

a. The Wire Third Party Query (WTPQ) system must capture audit data for each use of the system, as follows:

- The identity of the requester,
- The identity of the person on which the inquiry is made, and
- The date of the inquiry.

See DSHS IT Security References R11.2.1S5 Audit Trails for SSA Data.

b. The DSHS ACES SOLQ system must capture audit data for each use of the system, as follows:

- The identity of the initiator.
- The identity of the person on which the inquiry is made.
- Request Reason–Any necessary explanatory information such as the identity of the ACES client when the subject of the query is a different person e.g. a "community spouse".
- The time and date of the query.
- Whether the query or attempted query was against a Celebrity File or Congressional/Alien Social Security Number.

S6. Audit trail records must be “read” only with access restricted to “need to know” and must be retained for six years.

See DSHS IT Security Procedures P11.3.3 Retention Period for Log Pages.

S7. Other agencies that use WTPQ must have a data share agreement between the agency and the Social Security Administration. This agreement must be attached to the contract that permits the agency to use the DSHS WTPQ system.

S8. DSHS must submit to the SSA any significant architectural changes made to the system or to the system's security features for both WTPQ and SOLQ.

S9. Report any breaches of security or unresolved investigations involving social security information to the SSA.

11.3 POLICIES AND STANDARDS FOR SAFEGUARDING IRS TAX INFORMATION

The IRS requires stringent safeguards for protecting IRS tax information. The following standards augment other standards in this manual to comply with the provisions of IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.

11.3.1 IRS PHYSICAL SECURITY REQUIREMENTS

11.3.1.1 IRS Safeguards During Working Hours

Policy Statement 11.3.1.1

DSHS organizational units processing and/or using IRS tax information shall safeguard that information during working hours (during non-working hours see 11.3.1.2) by using one (or a combination) of the following secure facilities:

a. Restricted area.

b. Security room.

c. Secured work areas.

The criterion for each type of facility is set forth in IRS Publication 1075, Section 4.0.

Standards

S1. If a Restricted Area is dedicated to processing or storing IRS tax information: See DSHS IT Security Procedures P11.3.1.1.S1 Secured Room for Storing IRS Information.

a. Maintain a list of names of individuals authorized access to IRS tax information stored in the area.

b. Require anyone not assigned to the dedicated area to sign, in ink, a visitor's register at the entrance to the area. Information needed in the register includes:

- Visitor's name.
- Visitor's signature.
- Name of visitor's organization.
- Date and time of the visit.
- Purpose of the visit.

c. Supervisors shall review the log periodically to determine the need for access by each individual.

d. Cutoff log pages on June 30 each year, retain them for five years, and then destroy them.

e. Lock all entrances to the dedicated area, unless an employee assigned to work in the area is present.

f. Limit and log distribution of keys/key cards to the dedicated area.

See DSHS IT Security Procedures P11.3.7 Storing and Processing IRS Tax Information on PCs and Workstations.

S2. If a Non-Restricted Area is used for processing or storing IRS tax information:

a. The work area must be secure and protected from entry by the public. Locking devices, such as key cards or keypads, shall protect entrances to the work area.

b. Except when actually in use, IRS tax information shall be stored in lockable containers located within the secure work area.

c. Do not co-mingle tax documents with other documents.

11.3.1.2 IRS Safeguards During Non-Working Hours

Policy Statement 11.3.1.2

IRS regulations require that two locks, such as a locked metal container within a locked room, protect stored IRS tax information and that precautions be taken to protect keys, combinations, etc. This requirement applies to all references in other sections of this chapter to "store in a locked container".

Standards

S1. Organizations processing and storing IRS tax information will:

a. Limit and log distribution of keys/combinations, and maintain a list of key/combination holders.

b. Change keyed locks periodically. If a copy of a key cannot be accounted for, change the lock immediately.

c. Ensure that individuals who terminate employment or change duties return keys.

d. Change combinations to locks (doors and containers) at least annually, or when an employee in possession of the combination terminates employment or changes duties.

11.3.2 GENERAL SAFEGUARD REQUIREMENTS

Policy Statement 11.3.2

DSHS managers and supervisors who have responsibility for processing or handling IRS tax information must comply with the standards below. See DSHS IT Security References R11.3.2 Responsibilities of ISSD; DEAP; DCS.

Standards

S1. Restrict access to IRS tax information to those employees whose duties directly involve processing or using this information.

S2. Protect IRS tax information from access by clerical staff, couriers, and others who do not require access to IRS tax information in the execution of their duties.

S3. Brief employees on their responsibility for safeguarding IRS tax information when they are first assigned responsibility for processing or handling IRS tax information, and annually thereafter. See DSHS IT Security Procedures P11.3.2.S3 Employee Briefings.

S4. As a part of each briefing:

a. Provide each employee with a copy of the Employee Handout, Penalties for Unauthorized Disclosure of Tax Information and explain possible penalties associated with unauthorized disclosure of IRS tax information.

b. Require each employee to sign a completed DSHS 16-156, Statement of Understanding. For subsequent briefings, supervisors may use a memorandum, signed by the supervisor, listing all employees receiving the briefing at that time.

S5. Maintain a record of each briefing for five years, after which it may be destroyed. If a memorandum is used for subsequent annual briefings, the latest DSHS 16-156 form signed by the employee must be retained for five years after the employee's final annual briefing.

S6. Maintain a roster of all employees who have access to IRS tax information.

S7. Any hard copy document or report containing IRS tax information shall be recorded in a log [form approved by the DSHS IT Security Administrator] that identifies:

- Date received or created;
- Document identification e.g. number, date, and/or contents;
- Movement; and
- If disposed of, the date and method of disposition.

S8. Pulping, incineration or an approved shredder will destroy paper documents, including reports. A record of the destruction, including the method used, must be maintained on file for the current year and five previous years. A copy of this document must be forwarded to ISSD for inclusion in the annual Safeguard Activity Reports as follows:

a. By August 15 for Division of Employment and Assistance Programs (DEAP)

b. By December 15 for Division of Child Support (DCS)

See DSHS IT Security Procedures P11.3.2.S7 Destruction of Documents Containing IRS Tax Information.

S9. Documents/reports containing IRS tax information shall not be duplicated, photographed, or reproduced in any way.

11.3.3 SAFEGUARDING REMOVABLE MEDIA

Removable media includes magnetic tapes and cartridges; ZIP disks, CDs, etc., but excludes paper copies.

Policy Statement 11.3.3

DSHS managers and supervisors who have responsibility for processing or handling IRS tax information must comply with the standards below for logging, storing, and destroying removable media containing IRS tax information.

Standards

S1. All removable media containing IRS tax information that is created within DSHS must be clearly labeled, using an IRS Notice 129A label, as containing IRS tax information when created.

S2. Each item of removable media containing IRS tax information must be identified with a unique number to facilitate tracking and inventory processes.

S3. Form DSHS 16-155, Magnetic Tape/Disk – IRS Tax Data Log, or other form approved by the DSHS IT Security Administrator that meets the requirements of IRS publication 1075, rev. 6-2000, 3.2 Electronic Files, will be used to record the receipt, transfer, and destruction of all removable media containing IRS tax information

See DSHS IT Security Procedures P11.3.2.S7 Destruction of Documents Containing IRS Tax Information.

a. If an item logged on the form is transferred, the person receiving the item must sign the log showing receipt of the item.

b. If an item logged on the form has not been transferred and is subsequently destroyed, the log must be annotated showing the date and method of destruction and the name of the person performing the destruction.

c. Each log will be cut off for new entries on June 30 each year, retained for five years after completion of all entries, and then destroyed.

S4. All removable media containing IRS tax information must be stored in a metal, locked container when not in use or waiting transfer.

S5. All removable media containing IRS tax information must be inventoried every six months. A record of each inventory, showing the type of media, identification number, and who conducted the inventory will be retained on file for the current year and the five previous years. The party conducting the inventory must be from a different organizational entity than the

section responsible for storing and safeguarding the media.

See DSHS IT Security References R11.3.2 Responsibilities of ISSD; DEAP; DCS.

S6. All removable media containing IRS tax information must be destroyed when no longer needed, and a record of the destruction, including method used, must be annotated on the DSHS 16-155, Magnetic Tape/Disk – IRS Tax Data Log per instructions in Standard S3, above. Acceptable methods of destruction include:

a. Magnetic tapes and cartridges must be degaussed.

b. ZIP disks must be zero filled.

c. CDs must be incinerated or made unreadable by completely defacing the readable surface with rough sandpaper or similar course abrasives.

See DSHS IT Security Procedures P11.3.2.S7 Destruction of Documents Containing IRS Tax Information.

11.3.4 PROCESSING BEER INFORMATION

The Beneficiary and Earnings Exchange Record (BEER) files are received from the SSA via wire (Data Mover System). Files are received and initially processed on the Systems 390 mainframe, where they are immediately transferred to a tape (all references to tape in Section 11.3.4, may mean 9, 18, or 36-track tape), which is subsequently passed to DEAP for processing. See DSHS IT Security References R11.3.4 DEAP use of IRS Tax Information.

Policy Statement 11.3.4.1

DSHS managers responsible for receiving and processing incoming IRS information contained in the BEER files must adhere to the following safeguard standards.

Standards

S1. The BEER file will be transferred to a tape immediately following receipt from the SSA. The Systems 390 mainframe disk file used to receive and temporarily store the data must be zero filled and deleted immediately following the creation of the tape.

S2. The tape will be locked inside a locking box, within a locking cabinet. Only ISSD has the keys for these two locks. ISSD Operations will unlock both boxes, and pick up the tape. The tape will be logged into the DSHS 16-155, Magnetic Tape/DISK – IRS Tax Data log, and labeled, using an IRS Notice 129A label, as IRS Tax Information.

S3. The tape will be stored in ISSD Operations, within a doubly locked file cabinet, pending transfer to DEAP in accordance with the provisions of Section 11.3.3, above.

S4. The DEAP staff that picks up the tape will sign for each tape in the IRS Tax Data log.

S5. DEAP will convert the tape to ZIP disk files. After conversion, the tape must be degaussed and the logs annotated in accordance with the provisions of Section 11.3.3, above.

S6. ZIP disks must be logged (IRS Tax Data log), labeled, and safeguarded in accordance with the provisions of Section 11.3.3, above.

11.3.5 PROCESSING IRS UNEARNED INCOME TAX INFORMATION

The IRS tape (all references to tape in Section 11.3.5, may mean 9, 18, or 36-track tape) is received from the IRS by regular mail or Federal Express. The tape is converted to ZIP disk files by DEAP for subsequent processing. See DSHS IT Security References R11.3.4 DEAP use of IRS Tax Information.

Policy Statement 11.3.5

DSHS managers responsible for receiving and processing IRS unearned income tax information must adhere to the following safeguard standards.

Standards

S1. Log, label, and process tapes in accordance with the provisions of Section 11.3.3, above.

S2. Immediately degauss IRS tape D3, which is an unused error tape.

S3. Degauss remaining tapes after conversion to ZIP disks and annotate the log to reflect the destruction, including method used.

S4. Log, label, and process ZIP disks in accordance with the provisions of Section 11.3.3, above.

11.3.6 PROCESSING TAX REFUND OFFSET PROGRAM (TROP) INFORMATION

DCS receives the TROP file via wire (Data Mover System) through the Office of Child Support Enforcement (OCSE) in Washington, D.C. Files are received and initially processed on the Systems 390 mainframe, where they are immediately transferred to the UNISYS mainframe for subsequent processing by the Division of Child Support's (DCS) Support Enforcement Management System (SEMS). See DSHS IT Security References R11.3.6 DCS use of IRS Tax Information.

Policy Statement 11.3.6

DSHS managers responsible for receiving and processing TROP income tax information must adhere to the following safeguard standards.

Standards

S1. The TROP file will be transferred to the UNISYS mainframe for further processing immediately following receipt. The Systems 390 mainframe disk file used to receive and temporarily store the data must be zero filled and deleted immediately following the transfer. In addition, the UNISYS disk file shall be protected with an Access Control Record and zero filled and deleted when it is no longer needed.

S2. UNISYS batch files containing IRS tax information must be protected with Access Control Records and when no longer needed, zero filled and deleted.

S3. Disk files used to create CDs on the Systems 390 mainframe that contain IRS tax information must be zero filled immediately following creation of the CDs.

S4. ISSD Operations, immediately following notification by DIS, will collect the newly created IRS tax information CDs, and any defective copies created during the process.

a. Non-defective CDs must be logged, processed and stored pending transfer to DCS in accordance with the provisions of Section 11.3.3, above.

b. Defective CDs must be logged and immediately destroyed in accordance with the provisions of Section 11.3.3, above.

S5. Support Enforcement Management System (SEMS) printed reports containing IRS tax information will be printed in the secure ISSD Operations area. Any reports that must be disposed of by ISSD Operations due to printing errors or other reasons must be shredded (Section 11.3.2.S7.) Store reports in a locked container until picked up by the DCS courier or mailed to the appropriate DCS field offices by ISSD Operations.

Each report must be clearly marked as containing IRS tax information. In addition, each report must contain a one-page report control log that contains the following information:

- Report number
- IRS offset process year
- IRS offset process number
- DSHS run date (date report was created)
- A place for the signature/date of the person receiving the report

- A place for the signature/date of the person destroying the report
- A place to check the type of destruction.

Reports containing IRS tax information will not be duplicated, photographed, or reproduced in any way.

S6. Reports mailed to DCS field offices must be accompanied by a completed multi-copy DSHS Form 02-558, Transmittal Document – Reports Containing IRS Tax Information.

a. Report recipients must sign and date the form and return the original copy to ISSD Operations promptly. If the signed copy is not received by ISSD within seven working days from the date the report was mailed, ISSD Operations must initiate follow-up action.

b. ISSD will file their copy of Form DSHS 02-558. They will cut off the file on June 30 each year and destroy after five years.

c. DCS field offices will staple their copy of the Form DSHS 02-558 to the report control log. When the report is destroyed, complete the section on destruction, including method used, and file the log. Cut off the file on June 30 each year and destroy after five years.

S7. Reports shipped to DCS Headquarters via courier do not require a DSHS 02-558. Instead, a second copy of the control log is printed, and the courier must sign for the report on one copy that will be filed by ISSD Operations. ISSD Operations will cut off the file on June 30 each year and destroy after five years.

S8. Documents must be sealed in double, opaque envelopes, prior to distribution either by regular mail or courier, with both envelopes marked "TO BE OPENED BY ADDRESSEE ONLY." In addition, the inner envelope must be marked as “CONFIDENTIAL”.

11.3.7 SAFEGUARDING STANDALONE COMPUTERS CONTAINING IRS TAX DATA

Policy Statement 11.3.7

DSHS managers responsible for receiving and processing IRS tax information must adhere to the following safeguard standards as required in IRS Publication 1075.

Standards

S1. IRS tax information stored on computer hard drives must be protected as follows:

a. Access to the IRS tax information must be controlled by unique identification and authentication of users. The computer must be located in a secured facility (Section 11.3.1.1.S1); it must not be connected to a

network; and it must be dedicated for processing of IRS tax information. A system (CMOS) login password is sufficient for securing this environment.

b. An audit trail of user activities is required. A copy of audit trail files must be maintained for the current year and five previous years.

c. If a PC is removed for repair: See Chapter 3, Section 3.2.6 Special Procedures for Computer Hard Drives.

1. Over-write all databases/files containing IRS tax information with zeros and then delete the files, or

2. Remove and protect the hard drive before submitting the PC for repair.

11.3.8 SAFEGUARDING MAINFRAME DEVICES CONTAINING IRS TAX DATA

Policy Statement 11.3.8

DSHS managers responsible for receiving and processing IRS tax information must adhere to the following safeguard standards as required in IRS Publication 1075.

Standards

S1. IRS tax information stored on mainframe storage devices and/or transmitted over telecommunications devices must be protected as follows:

a. Access to the IRS tax information must be controlled by unique identification and authentication of users.

b. An audit trail of user activities to ensure that user actions are within established controls is required. A copy of audit trail files must be maintained for the current year and five previous years.

c. IRS tax information transmitted over telecommunications devices must be encrypted unless the transmission is over guided media (protected microwave transmissions or end-to-end fiber optics). In addition, copper cable may be used where the cable is adequately protected (locked switching rooms, cable buried underground, etc.).

11.3.9 INTERNAL INSPECTIONS

DSHS is required by IRS Publication 1075, Section 6.3, to conduct periodic inspections during the year to ensure that safeguards are adequate. The department satisfies this requirement using internal professional auditing staff to perform an annual audit of the department's compliance with the provisions of the DSHS IT Security Manual and IRS Publication 1075. (See Chapter 9, Security Assessments, Reviews, and Reports).

11.3.10 ANNUAL SAFEGUARD ACTIVITY REPORTS

The DSHS CIO has responsibility for the preparation and submission of the annual Safeguard Activity Reports for DCS and DEAP as required by IRS Publication 1075. (See Chapter 9, Security Assessments, Reviews, and Reports).

11.4 DEAP QUALITY CONTROL (QC) PROCEDURES

11.4.1 PROCESSING IRS "HIT" INFORMATION

Policy Statement 11.4.1

DEAP QC managers have responsibility for ensuring that the following standards for complying with IRS safeguard requirements are complied with.

Standards

S1. Computer printouts containing confidential IRS tax information will be stored in the DEAP restricted area and destroyed when obsolete.

S2. Each document with "hit" information will be assigned an identification number, and labeled as IRS Tax Information, by the headquarters QC staff. The identification number will facilitate tracking a document containing "hit" information from the time it is created until it is destroyed.

S3. Prior to mailing hit information to the QC field offices:

a. Documents must be logged in the Headquarters QC Unit - Tax Information Log.

b. Documents must be sealed in double, opaque envelopes with both envelopes marked "TO BE OPENED BY ADDRESSEE ONLY." In addition, the inner envelope must be marked as “CONFIDENTIAL”.

S4. Upon receipt of "hit" information, the QC secretary will: (See DSHS IT Procedures, P11.4.1.S4: Processing “Hit” Information by DEAP QC Field Offices.)

a. Record each document in the QC Field Unit - Tax Information Log

b. Store the document in a locked container until no longer needed.

c. When returning documents for destruction, log the document in the QC Field Unit - Tax Information Log as being returned to Headquarters QC staff.

S5. Upon receipt of the returned "hit" information, Headquarters QC staff will:

a. Log receipt of the document in the Headquarters QC Unit - Tax Information Log.

b. Destroy the document by shredding and record the destruction, including the method used, in the Headquarters QC Unit - Tax Information Log.

S6. Each log page, of both the Headquarters QC Unit - Tax Information Log and the QC Field Unit - Tax Information Log, will be cut off for new entries on June 30 each year, retained for five years after the completion of all entries, and then destroyed.

11.5 INTERNAL DCS PROCEDURES

DCS internal procedures for safeguarding IRS tax information are contained in DCS Administrative Policy 7.01, IRS Confidentiality and Security.

Chapter 12: Mainframe and MAPPER Security

12.1 INTRODUCTION

A. This chapter contains policies and standards governing access to the UNISYS and System 390 mainframe applications and processes. It also covers MAPPER security.

B. The term "ISSD mainframe data security staff" is a collective term used to denote all ISSD staff involved in administering access security to both the UNISYS and System 390 mainframes.

12.2 POLICIES AND STANDARDS FOR THE UNISYS MAINFRAMES

This Section addresses policies and standards unique to UNISYS mainframe security. See Chapter 4, Access Security, Identification, and Authentication, for policies and standards relating to login ids and changing and resetting passwords. For additional information on UNISYS transactions and security, see DSHS IT Security References R12.2 UNISYS.

12.2.1 TRANSACTION PROCESSING (TIP) SECURITY

Transaction processing (TIP) allows online/real-time processing of transactions from remote terminals. For additional information on TIP transactions and security, see DSHS IT Security References R12.2.1 Description of Online TIP Transactions.

Policy Statement 12.2.1

ISSD mainframe data security staff shall administer TIP transaction security on the UNISYS Mainframe and take necessary steps to prevent unauthorized additions, changes, or deletions to PID and operator records designating operator's privileges.

Standards

S1. ISSD Mainframe Data Security will administer TIP access security for the department on behalf of the program areas owning the TIP applications.

S2. ISSD Mainframe Data Security will accept requests for additions, changes, or deletions to TIP access security only from program managers owning the applications or ISSD Help Desk.

S3. The security record of each PID must identify only those TIP transactions authorized to be executed from the PID.

S4. Each Operator record must contain only the subset of PID TIP transactions that the operator is authorized to execute.

S5. ISSD Mainframe Security staff shall exercise due diligence to ensure that, when cloning PID and operator records, unauthorized transactions are not transferred to the new records.

S6. Automatic sign-on will be set to off for all PID records, except for terminals that are used by multiple staff, in which case such terminals must be located in a secure work area protected from the public.

S7. The hours during the allowable days (above) when users can log terminal(s) on to the system will be set to the standard access hours of 6:00 a.m. to 6:00 p.m. Program managers may be granted permanent exceptions upon request, providing the associated terminals will be used on a routine basis during the extended period of coverage.

S8. ISSD Mainframe Data Security staff has responsibility for registering TIP programs in VALTAB at the request of the application programmer.

S9. Terminals may be shared among staff who input/update transactions for SSPS and staff who do inquiries for other systems. The following applies when non-SSPS staff and SSPS staff must share a terminal:

a. Non-SSPS staff without an individual operator number must use the shared operator number assigned to each division, and the standard password from a list maintained by the ISSD Help Desk.

b. SSPS staff shall use their individually assigned operator numbers.

12.2.2 ADMINISTERING CONTROL OF DEMAND ACCESS

Demand access is an online process that allows data processing staff to create, review, modify, and delete program and data files on the UNISYS mainframes. For more information, see DSHS IT Security References R12.2.2 Demand and Batch Access.

Policy Statement 12.2.2

ISSD Mainframe Data Security staff is responsible for administering demand access to the UNISYS Mainframe by DSHS employees.

Standards

S1. ISSD Mainframe Security staff will:

a. Use Site Management (SIMAN) software to control demand access to the production and development UNISYS mainframes.

b. Limit demand access to the UNISYS development mainframe to IT staff who have a need to develop and test applications.

c. Limit demand access to the UNISYS production mainframe to IT and operations staff whose duties include:

- Call-back for maintenance of critical applications systems
- Maintenance of production libraries
- Staging or de-staging of production jobs
- Maintenance of production databases

12.2.3 UNISYS MAINFRAME SECURITY OPTION 1 (SECOPT1)

SECOPT1 is available on the UNISYS mainframes for protecting flat files and tape volumes. SECOPT1 is necessary for protecting department applications from access by other agencies sharing these mainframes. For additional information, see DSHS IT Security References R12.2.3 File and Subsystem Security.

Policy Statement 12.2.3

Departmental organizations using the UNISYS mainframes will use Access Control Records (ACRs), a feature of SECOPT1, to protect flat files and tape volumes located on these mainframes.

Standards

S1. Programming staff will use the ACR feature of SECOPT1 to protect all flat files and tape volumes located on the UNISYS mainframes for which they have responsibility.

12.3 POLICIES AND STANDARDS FOR THE DIS SYSTEM 390 MAINFRAMES

DSHS uses the DIS System 390 mainframes (IBM and AMDHAL) as well as the ACES IBM mainframe to process applications. Resource Access Facility (RACF) front-end security software is used to control access to applications and data residing on all mainframes in this category. See Chapter 4, Access Security, Identification, and Authentication, for policies and standards relating to login IDs and changing and resetting passwords. For additional information on RACF Security, see DSHS IT Security References R12.3 IBM System 390.

12.3.1 RACF SECURITY ADMINISTRATION

The RACF security administrator is a member of the ISSD Mainframe Security staff.

Policy Statement 12.3.1

ISSD Mainframe Data Security staff has responsibility for administering RACF security for all DSHS applications.

Standards

S1. The Chief, ISSD Operations, will appoint a RACF Security Administrator, and backups as appropriate, to administer RACF security for DSHS.

S2. The RACF Security Administrator will create, update, and delete all users, as needed.

S3. Divisions may appoint security sub-administrators in Natural to add, update, and delete users, but it is not mandatory to do so. The department's RACF Security Administrator will furnish access security service if Natural administrators are not used.

S4. The RACF Security Administrator is responsible for Natural security to outside agency systems used by DSHS staff.

12.4 POLICIES AND STANDARDS FOR MAPPER

MAPPER is a multi-platform development system administered by DSHS-ISSD MAPPER Administrators (Click here for MAPPER Procedures maintained by the DSHS MAPPER Administrator.) Applications and/or data are organized in MAPPER "departments." MAPPER applications currently run on Microsoft Windows server platforms. A MAPPER department owner is also called a MAPPER sub-administrator.

See Chapter 7, Access Security and Identification and Authentication, for policies and standards relating to login IDs and changing and resetting passwords.

12.4.1 RESPONSIBILITIES OF MAPPER ADMINISTRATORS

Policy Statement 12.4.1

The DSHS-ISSD MAPPER Administrator and program area MAPPER sub-administrators have responsibility for creating MAPPER departments and controlling user access.

Standards

S1. DSHS-ISSD MAPPER Administrators shall coordinate the establishment and removal of MAPPER departments, databases, and MAPPER communications, and the changing of department owners.

S2. The MAPPER department owner (sub-administrator), shall:

a. Coordinate all requests for establishing and removing MAPPER departments, databases, and MAPPER communications with the DSHS MAPPER Administrator.

b. Be responsible for granting access to the department under his or her control.

Glossary

ACES

The Automated Client Eligibility System or the organization by the same name within the Economic Services Administration.

BACKDOOR

A backdoor is a program that opens secret access to systems, and is often used to bypass system security. A Backdoor program does not infect other host files, but nearly all Backdoor programs make registry modifications.

CIO

The Department's Chief Information Officer.

CMOS

There are a number of methods to prevent booting from a floppy disk, ranging from physical disk locks to purchased security programs. But the simplest solution is to use the security that is already built into the computer by enabling the computer's CMOS security features.

The CMOS is a storage area on the PC where information is retained even when the power is turned off. Important information is stored here about the computer, and is accessed by a special CMOS setup program.

CARETAKER

A caretaker of data is that management position with primary responsibility and accountability for the integrity of data and authority over access to it.

CLASSIFIED DATA OR CLASSIFIED INFORMATION

We have assigned a special meaning to the terms "classified data" and "classified information" by using them to collectively denote categories 2 through 4 of the four standard categories of data defined at IT Security Policy Manual, Section 3.2.1, "Classify Data According to Level of Protection Needed", i.e "Sensitive Information", "Confidential Information", and "Information Requiring Special Handling".

CONFIDENTIAL INFORMATION

Confidential information is information that is specifically protected by law. It generally includes:

a. Personal information about individual clients, regardless of how that information is obtained.

b. Information concerning employee payroll and personnel records.

c. Source code of certain applications programs that could jeopardize the integrity of department data or result in fraud or unauthorized disclosure of information if unauthorized modification occurred.

CONFIDENTIALITY

We use "confidentiality" as a generic term meaning the limitation of disclosure of information.

DENIAL OF SERVICE ATTACK

From CERT Coordination Center Article

1. A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

    - attempts to "flood" a network, thereby preventing legitimate network traffic
    - attempts to disrupt connections between two machines, thereby preventing access to a service
    - attempts to prevent a particular individual from accessing a service
    - attempts to disrupt service to a specific system or person

Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack.

Illegitimate use of resources may also result in denial of service. For example, an intruder may use your anonymous ftp area as a place to store illegal copies of commercial software, consuming disk space and generating network traffic.

DEPARTMENT PERSONNEL

Defined at Chapter 2 Personnel and Use of State Resources, section 2.1.B to include permanent, temporary, and contract personnel or other users who:

1. Have responsibility for or access to department data;
2. Use or have access to department information technology (IT) equipment or other IT resources; or
3. Are engaged in developing, coding and testing information systems for the department.

ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

Protected Health Information (PHI) that is stored or transmitted in electronic form. PHI is defined at Administrative Policy 5.01 Privacy Policy -- Safeguarding Confidential Information as “Individually identifiable health information about a client that is transmitted or maintained by DSHS…Individually identifiable health information in DSHS records about an employee or others who are not clients is not protected health information.”

HIPAA

Federal Health Insurance Portability and Accountability Act

INFORMATION REQUIRING SPECIAL HANDLING

Information requiring special handling is information for which:

a. Regulations or agreements dictate especially strict handling requirements; or

b. Serious consequences could arise from unauthorized disclosure ranging from life threatening to legal sanctions.

ISSD

Information System Services Division. The current director of ISSD is also the Department's Chief Information Officer (CIO).

IT RESOURCES

All computing and telecommunications facilities, hardware, software and personnel.

MANAGERS

The person(s), at any level of management, who are responsible for a given organization within DSHS. This could be an Assistant Secretary, a Division Director, an Office Chief, etc.

PROTECTED HEALTH INFORMATION (PHI)

PHI is defined at Administrative Policy 5.01 Privacy Policy -- Safeguarding Confidential Information as “Individually identifiable health information about a client that is transmitted or maintained by DSHS in any form or medium. Individually identifiable health information in DSHS records about an employee or others who are not clients is not protected health information.”

PUBLIC INFORMATION:

Public information is information that can be released to the public. It does not need protection from unauthorized disclosure, but does need protection from unauthorized change that may mislead the public or embarrass DSHS.

SAM

The Microsoft Security Accounts Manager (SAM) is the standard access control system that is included as part of the Windows NT/2000/XP operating systems.

SENSITIVE INFORMATION:

Sensitive information is not specifically protected by law, but should be limited to official use only.

SOCIAL ENGINEERING

An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) he needs to gain access to the system.

A classic social engineering trick is for a hacker to send email claiming to be a system administrator. The hacker will claim to need your password for some important system administration work, and ask you to email it to him/her. It's possible for a hacker to forge email, making it look like it came from somebody you know to be a legitimate system administrator. Often the hacker will send this message to every user on a system, hoping that one or two users will fall for the trick.

STATE GOVERNMENTAL NETWORK (SGN)

Another name for Statewide Area Network (see below)

STATEWIDE AREA NETWORK (DIS WAN)

Department of Information Systems Wide Area Network (also referred to as "the department's trusted Wide Area Network (WAN)"): the telecommunications network that links state agency offices throughout the state.

SYSTEM

A system is

- one or more applications that perform related business function(s) on one or more related databases; or
- a collection of one or more related runs that have a beginning and end to their processing cycle and include all programs and files involved in the cycle.

Within any system the related IT functions of create, retrieve, update, and delete are performed.

VOUCHER SYSTEM

The voucher system is currently being developed by the Certificate Authority (Digital Signature Trust - DST) and the Department of Information Services. Until this system is available, requests certificates by contacting the IT Security Administrator . He will provide details on acquiring a certificate(s).

DST Voucher System - Program Areas must use DST vouchers, obtained through the ISSD Digital Certificate Tracking and Reporting System, to purchase and renew digital

certificates from DST. The use of vouchers, in conjunction with the ISSD Digital Certificate Tracking and Reporting System, simplifies and facilitates the centralized tracking and reporting functions performed by ISSD.

ISSD will purchase vouchers from DST (one voucher per certificate) for a $5.00 deposit for each voucher. A voucher is valid for all certificates, including server certificates, and related hardware and software. DST will bill ISSD for the actual certificate price minus the $5.00 voucher deposit.

To purchase or renew certificates, organizations will secure the appropriate number of vouchers from ISSD, and then work directly with DST, via their online system, to actually secure the certificates.